# EXHIBIT D

# Trend Micro Security 2021 for Windows

# Product Guide

**Trend Micro™ Antivirus+ Security**

**Trend Micro™ Internet Security**

**Trend Micro™ Maximum Security**

V1.0

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before implementing the product, please review the readme file and the latest version of the applicable user documentation.

Trend Micro, the Trend Micro t-ball logo, Titanium, and Trend Micro Security are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2020 Trend Micro Inc., Consumer Technical Product Marketing. All rights reserved.

*Trend Micro™ Security 2021 Product Guide for Windows* provides help for analysts, reviewers, potential customers, and users who are evaluating, reviewing, or using the 2021 (v17) version of Trend Micro™ Antivirus+ Security, Trend Micro™ Internet Security, or Trend Micro™ Maximum Security on the Windows platform. The products are understood to be the most recent editions (2021, v17), even when "2021" or "v17" are not designated.

This product guide can be read in conjunction with its companion guides, which can be accessed from the Home Support/Product Support dropdown menu, as well as from the individual links below:

- Trend Micro™ Antivirus for Mac® Product Guide
- Trend Micro™ Mobile Security for Android Product Guide
- Trend Micro™ Mobile Security for iOS Product Guide
- Trend Micro™ Password Manager for Windows and Android Product Guide
- Trend Micro™ Password Manager for Mac and iOS Product Guide

DOCUMENT PROFILE:

Product: Trend Micro™ Security 2021 for Windows

Document Title: Trend Micro™ Security 2021 for Windows – Product Guide

Document Filename: PG - TM Security 2021 for Windows - Product Guide v1.0

Document Release Date: October 21, 2020

Team: Consumer Technical Product Marketing

# Table of Contents

Chapter 1: Introduction to Trend Micro™ Security ..... 6
The Trend Micro™ Security Family ..... 6
Trend Micro Security Highlights ..... 7
Key Features of Trend Micro Security ..... 11
System Requirements ..... 12
Internet Connection, USB Installation ..... 14
Target Audience ..... 14
Global Availability ..... 14
Contacting Trend Micro ..... 14
Consumer Support Line ..... 14
Free Phone, Email and Chat support ..... 15
Premium Support Services ..... 15
Chapter 2: Installing and Activating Trend Micro Security ..... 16
Install Trend Micro Security ..... 16
Explore More Features – Questionnaire and Wizard ..... 29
Protect Another Device ..... 32
Set Up Folder Shield ..... 39
Install Trend Micro Security for Microsoft Edge ..... 41
Web Threat Protection ..... 44
Fraud Buster for Gmail and Outlook Webmail ..... 45
Ad Block ..... 48
Privacy Scanner ..... 49
Pay Guard ..... 50
Password Manager ..... 52
Enable/Disable Trend Micro Security for Edge ..... 54
Install Trend Micro Toolbar for Google Chrome, Mozilla Firefox, or Internet Explorer ..... 55
Rate Links on Web Pages ..... 60
Rate Links on Mouseover ..... 61
Fraud Buster for Gmail and Outlook Webmail ..... 63
Check Your Online Privacy ..... 66
Open in Pay Guard ..... 66
Settings ..... 68
Help ..... 69
Enable/Disable Trend Micro Toolbar ..... 69
Set Up Parental Controls ..... 70
Chapter 3: Trend Micro Security Overview ..... 71
Quick Start: The Trend Micro Security Console ..... 71
Quick Start: Conducting On-Demand Scans ..... 71
Scan Your Computer's Disk ..... 72
Quick Scan and Full Scan ..... 73
Custom Scan ..... 74
Intensive Scan ..... 75
Quick Start: Viewing Security Reports ..... 76

Chapter 4: Trend Micro Antivirus+ Security ..... 80
Protection Overview ..... 80
Device: Security Settings: Security & Tuneup Controls > Scan Preferences ..... 82
Device: Security Settings: Security & Tuneup Controls > Scheduled Scans ..... 85
Device: Security Settings: Internet & Email Controls > Web Threats ..... 86
Device: Security Settings: Internet & Email Controls > Spam & Emailed Files ..... 87
Device: Security Settings: Internet & Email Controls: Network > Firewall Booster | Wi-Fi Protection ..... 94
Exception Lists: Programs/Folders ..... 95
Exception Lists: Websites ..... 96
Exception Lists: Wireless Connection ..... 97
Other Settings: System Startup ..... 98
Other Settings: Network Settings ..... 99
Other Settings: Smart Protection Network ..... 100
Other Settings: Password ..... 101
Other Settings: Background and Animation ..... 101
Device: Mute Mode ..... 105
Device: Protect Another Device ..... 108
Privacy: Social Networking Protection ..... 108
Privacy: Pay Guard ..... 112
Data: Folder Shield ..... 116
How Folder Shield Works ..... 121
Family: Upgrade Now ..... 124
Chapter 5: Trend Micro Internet Security ..... 126
Protection Overview ..... 126
Device: Security Settings: Security & Tuneup Controls > Smart Scheduled Scan ..... 130
Device: PC Health Checkup | Security Settings ..... 132
Perform a PC Health Checkup ..... 132
Configure PC Health Checkup ..... 134
Security Report: PC Health Checkup ..... 135
Device: Protect Another Device ..... 138
Privacy: Privacy Scanner: Social Network Privacy & Web Browser Privacy ..... 138
Facebook Privacy Settings ..... 140
Facebook App Privacy Settings ..... 143
Twitter Privacy Settings ..... 144
LinkedIn Privacy Settings ..... 146
Web Browser Privacy Settings ..... 149
Privacy: Data Theft Prevention ..... 151
Data: Secure Erase ..... 154
Data: Password Manager - Free Trial ..... 156
Family: Parental Controls ..... 165
Security Report: Parental Controls ..... 177
Chapter 6: Trend Micro Maximum Security ..... 180
Protection Overview ..... 180
Device: Protect Another Device ..... 181
Data: Password Manager - Full Version ..... 181
Install Password Manager in Pay Guard ..... 189

Using Password Manager ..... 191
Data: Vault ..... 193
Chapter 7: Trend Micro Security: Explore More Features, Get Help, Identity, and Tools ..... 198
Explore More Features ..... 198
Help > Product Support ..... 199
Help > Premium Services ..... 200
Help > Ransomware Help ..... 201
Help > Feedback ..... 202
ID > Account ..... 203
ID > Subscription Information ..... 204
ID > About the Software ..... 205
The Trend Micro Tools ..... 207
About Trend Micro ..... 212

# Chapter 1: Introduction to Trend Micro™ Security

Trend Micro™ Security secures your connected world, providing protection against malware, ransomware, and online banking threats. Using advanced artificial intelligence, it also helps protect you from identity theft, coin-mining and file-less malware, viruses, online tech support and phishing scams, and other emerging threats.

Trend Micro Security offers multi-device protection and includes robust Parent Controls to help keep your kids safe online, a Password Manager to protect and manage passwords, and a Privacy Scanner to secure your privacy on social media. Its enhanced Folder Shield feature keeps your valuable files safe from ransomware by allowing only authorized applications to have access to protected folders, whether stored locally or synced online. It also provides Pay Guard, a protected web browser, that adds an extra layer of protection when banking or shopping online. And its Advanced Artificial Intelligence capability, which can stop unknown threats in their tracks, works with other key, layered technologies to provide the best and deepest security in the industry.

With 30+ years of internet security leadership, Trend Micro keeps millions of users safe from harm. As attested by AV-TEST, one of the world's premium security software testing labs, the product is one of the best on the market. At the beginning of 2019, Trend Micro Internet Security Received a **Best Protection Award** *for the whole of 2018*. See *AV-TEST Awards 2018 Go To Trend Micro*.

And it consistently receives a **Top Product Certification** for its protection, as recently attested in the *AV-TEST Product Review and Certification Report – May-Jun/2020*.

Indeed, working hard to protect its users from harm, Trend Micro's Smart Protection technology blocks more than *250 million threats every day.*

## The Trend Micro™ Security Family

The family of **Trend Micro™ Security** products includes the following:

- **Trend Micro™ Antivirus+ Security.** Our entry-level product keeps you safe online while you work and play. Antivirus+ Security alerts you to dangerous ransomware threats in web searches and emails. Also, it gives you simple screens and clear, easy-to-understand security status reports. You can protect 1 Windows® PC.
- **Trend Micro™ Internet Security**. Our mid-range product provides advanced online protection for up to 3 Windows® PCs. It keeps you safe online while you socialize, browse, work, and play. It also helps safeguard your privacy on social networks. Internet Security alerts you to dangerous ransomware and other threats in web searches and emails. Parental controls are included to help keep children safe online.
- **Trend Micro™ Maximum Security**. Our high-end product provides comprehensive, multiple device protection so you can enjoy your digital life safely. It keeps you safe

while you socialize, browse, work, and play online. It safeguards against viruses and ransomware, dangerous websites, and identity theft. It also helps you secure your privacy on social networks. You can use Maximum Security to keep kids safe online and protect your passwords. Additionally, you have the flexibility to protect 5 to 10 devices, depending on your subscription – for any combination of PC, Mac, or mobile.

- **Trend Micro™ Antivirus for Mac®.** Industry experts know that Macs are no longer immune to viruses and other Internet threats. As a Mac user, you need privacy protection when shopping, banking and socializing online. Antivirus for Mac® provides online privacy and protection so you can enjoy your digital life safely. It shields you from Internet threats, dangerous websites, and phishing that can lead to identity theft. It also helps you guard your privacy on Facebook, Twitter, and LinkedIn.

# Trend Micro Security Highlights

Trend Micro Security is equipped with special protection features and is bundled with companion products to address specific needs:

### New or Improved Features

- **Operating System Compatibilities.** The Trend Micro Security Family is compatible with Windows 10, Android, MacOS, and iOS. The Trend Micro Toolbar is also available for Windows 10 S Mode and for Chrome OS on Chromebooks.
- **On-Boarding Help.** Trend Micro Security helps users get onboard with important security options through new assistance tools such as Explore More Features, Protect Another Device with easy Mobile Security installation, and easier Trend Micro Toolbar and Pay Guard enablement.
- **Improved Notifications.** Improved notifications include Game Compatibility tests, a Download File Scan popup, and an enhanced Mute Mode Status notification.

### Highlights

- **Fraud Buster.** Scam webmail that contains no malicious URLs or attachments, but which is nonetheless dangerous, is undetected by traditional email security technology. Trend Micro's Fraud Buster for Gmail and Outlook Webmail is developed to deal with this type of scam. It utilizes AI to identify the topic and to understand the intention of the scam email and warns you against it upon discovery. You can then delete it with confidence.
- **PC Health Checkup** – Now with enhanced Potentially Incompatible Program (PIP) detection, Trend Micro Security provides additional performance optimization for your PC. Powered by Trend Micro's Platinum technology, you can check for PIPs, security vulnerabilities, and clean up unneeded files to boost your performance.
- **Pay Guard.** Trend Micro Security's protected web browser adds an extra layer of protection when you're banking or shopping online with Edge, Chrome, Firefox, or Internet Explorer. You can now launch Pay Guard directly from Trend Micro Security for Edge or the Trend Micro Toolbar, so its powerful protection features are more easily applied to your default browser automatically, protecting all the data in your financial transactions, including credit card information and personal data.

- **Gamer-Friendly Mute Mode.** Mute Mote lets you temporarily stop non-critical notifications while you're gaming or doing an important task, so you're not distracted. Game compatibility has been enhanced, as well as auto-enablement, and you can now set a specific time-limited for Mute Mode, which will automatically turn off when the time interval has expired.
- **Coin-mining Malware Protection**. Trend Micro Security can protect you against the latest coin-mining malware, which can hijack your computer's resources to secretly mine cryptocurrencies.
- **Fileless Malware Protection**. Trend Micro Security provides improved protection against fileless malware infections from spam campaigns or malicious websites, which can alter the Windows Registry and execute in Windows PowerShell, delivering malicious payloads that execute within memory.
- **Tech Support and Phishing Scams.** Protects against automated online scams that alert you with phony warnings in emails or when browsing to fake infections, or prompt you to call fraudulent tech support hotlines for purposes of hijacking your computer, to steal your identity data or your money.
- **Enhanced Folder Shield.** Enhances Trend Micro Security's ransomware protection by extending it to every user account on your computer. Protects your key documents from modification by malware or encryption by ransomware. You can customize which folders and files are protected and can include folders synced to Microsoft OneDrive, Google Drive, or Dropbox.
- **Network Scan.** You can now scan your network to detect unprotected devices, to alert you where you should install the unused seats in your multi-device license, to protect other members of your family.
- **Artificial Intelligence**. It's all about making the unknown known. With its evolutionary, hybrid blend of the latest threat protection techniques and infused machine learning, Trend Micro's artificial intelligence capability, active in Trend Micro Security, is always adapting to identify and defeat new ransomware and other unknown threats.
- **Trend Micro Troubleshooting Tool.** Our enhanced **Troubleshooting Tool** makes it quick and easy for Trend Micro Support Professionals to make repairs and fix problems.

**Privacy Protection and Social Networking Security**

- **Privacy Protection for Facebook, Twitter, and LinkedIn.** Trend Micro Security features an easy-to-use Privacy Scanner for social media, which identifies privacy settings that may leave your personal information publicly available and vulnerable to identity theft. Facebook applications are also scanned and the user warned if the app is posting with too wide of an audience.
- **Privacy Protection for Browsers.** Privacy Protection is provided for leading PC browsers. A simple scan of Google Chrome, Internet Explorer, or Mozilla Firefox helps increase your privacy when browsing the web.
- **Facebook Application Privacy Scanner.** Scans Facebook applications used and warns if the app is posting to your wall with too wide of an audience (Public).

- **Social Networking Security (SNS) Protection.** Trend Micro Security provides protection from threats you may encounter from malicious links in Facebook, Twitter, MySpace, LinkedIn, Pinterest, Mixi, and Sina Weibo—the broadest and most effective SNS protection available on the market for consumers today.
- **Clear Warning.** Our SNS proactively warns you when a link is bad by highlighting it in red. When it's a safe link, it's highlighted in green. You can also mouse over a link to get real-time details about its safety from our Web Threat Protection servers.
- **Warn a Friend.** Trend Micro Security even allows you to easily and quickly inform your Facebook friends when it identifies a malicious link, so they can delete it from their Facebook page.

**Family Protection**

- **Parental Controls** let you restrict your kids' usage of the Internet and prevent them from visiting inappropriate websites, now including blogs/web communications and protection from illegal drugs. Enhanced functions include program restrictions, which can be set by schedule; safe search filtering, which helps prevent adult content from appearing in search results; and blocking of untested websites, to increase security when browsing.

**Data Theft Prevention**

- **Data Theft Prevention (DTP).** DTP lets you stop specific data, such as email accounts or credit card numbers, from being shared in Outlook outward-bound email or online forms.
- **Secure Erase** lets you overwrite and delete data from your disk, so it can't be recovered.
- **Vault** lets you encrypt data on your hard drive and remotely lock it up if your laptop is lost or stolen; when the device is found you can then unlock that data.
- **Trend Micro™ Password Manager** helps you securely store all your passwords and sensitive information, so you can access them when needed on PCs, Macs, and Android and iOS mobile phones and tablets. It's automatically installed with Trend Micro Maximum Security, so you can get started easily, or you can purchase it separately.

**Other Highlights**

- **Smart Scheduled Scan** – Trend Micro Security provides a Smart Scheduled Scan. Based on recent computer usage, the most suitable scan will start automatically at an appropriate time.
- **Screen Reader –** Screen Reader support is now available for visually-impaired users.
- **Intensive Scan Switch** – Automatically increases the protection level only when you need it – for intensive scans when your computer is infected.
- **Search Results Rating –** When you conduct a search on the internet the search results give you a list of URLs, proactively highlighted.

- **Manual URL/Link Scanner –** As with SNS, when you hover your mouse over a link in search results, the manual link scanner rates the safety and reputation of any links on the web page.
- **Mobile Security for Android and iOS** – Trend Micro Maximum Security includes Trend Micro Mobile Security for Android and iOS, for protection of your mobile devices.
- **Windows 10 compatibility –** Trend Micro Security is fully compatible with Microsoft's Windows 10 operating system, with backwards compatibility with Windows 8.1 and 7. See System Requirements for details.

**Clean User Interface**

- **Easy to Use.** Trend Micro Security provides a clean interface design. Both easy-to-use and powerful, the Trend Micro Security Console provides all the tools you need at the touch of mouse or a tap of a finger to easily configure your solution to meet your security needs. Conduct scans and obtain reports that let you know just how Trend Micro Security is protecting you.

# Key Features of Trend Micro Security

**Table 1. Trend Micro Security 2021 (v17) - Key Features**

| TREND MICRO SECURITY 2021 – Key Features | Trend Micro Antivirus for Mac | Trend Micro Antivirus+ Security | Trend Micro Internet Security | Trend Micro Maximum Security |
|---|---|---|---|---|
| Licensing | 1 user<br>Mac only | 1 user<br>PC only | 3 users<br>PC & Mac | 5 / 10 users<br>PC, Mac & Mobile |
| Pricing | $39.95/yr | $39.95/yr | $79.95/yr | 5 - $89.95/yr<br>10 - $99.95/yr |
| Virus and Spyware Protection | ✓ | ✓ | ✓ | ✓ |
| Rootkit Detection and Removal | | ✓ | ✓ | ✓ |
| Web Threat Protection | ✓ | ✓ | ✓ | ✓ |
| Anti-Spam | ✓ | ✓ | ✓ | ✓ |
| Anti-Phishing | ✓ | ✓ | ✓ | ✓ |
| Ransomware Protection | ✓ | ✓ | ✓ | ✓ |
| AI / Machine Learning | ✓ | ✓ | ✓ | ✓ |
| Auto Intensive-level Protection Scan Switch | | ✓ | ✓ | ✓ |
| Authenticate Wi-Fi Networks and Hotspots | | ✓ | ✓ | ✓ |
| Windows Firewall Booster | | ✓ | ✓ | ✓ |
| Block Malicious Links in Email | ✓ | ✓ | ✓ | ✓ |
| Search Results Ratings | ✓ | ✓ | ✓ | ✓ |
| Gamer-Friendly Mute Mode | | ✓ | ✓ | ✓ |
| Social Networking Protection | ✓ | ✓ | ✓ | ✓ |
| Smart Schedule Scan | | | ✓ | ✓ |
| Privacy Scanner:<br>Facebook, Twitter, LinkedIn; Facebook Applications<br>Internet Explorer, Google Chrome, Mozilla Firefox, Microsoft Edge (WIN) | ✓ | | ✓ | ✓ |
| Folder Shield | ✓ | ✓ | ✓ | ✓ |
| Fraud Buster | | ✓ | ✓ | ✓ |
| Pay Guard | | ✓ | ✓ | ✓ |
| Data Theft Prevention | | | ✓ | ✓ |

**Table 2. Trend Micro Security 2021 – Key Features (Continued)**

| TREND MICRO SECURITY 2020 – Key Features | Trend Micro Antivirus for Mac | Trend Micro Antivirus+ Security | Trend Micro Internet Security | Trend Micro Maximum Security |
|---|---|---|---|---|
| Secure Erase | | | ✓ | ✓ |
| PC Health Checkup | | | ✓ | ✓ |
| Vault with Remote File Lock | | | | ✓ |
| Password Manager with Integrated Installer / Activation | | | | ✓ |
| Parental Controls | ✓ | | ✓ | ✓ |
| Android | | | | ✓ |
| iOS | | | | ✓ |
| MacOS | ✓ | | | ✓ |

*Trend Micro Maximum Security provides seats for Windows, MacOS, Android, and iOS

# System Requirements

**Table 3. Trend Micro Antivirus+, Internet, and Maximum Security 2021**

| Operating System | CPU | Memory | Disk Space |
|---|---|---|---|
| Windows® 10, (32 or 64-bit) | 1 GHz | 2 GB (32-bit)<br>2 GB (64-bit) | 2.2 GB<br>2.5 GB Recommended |
| Windows® 8.1 (32 or 64-bit) | 1 GHz | 1 GB (32-bit)<br>2 GB (64-bit) | |
| Windows® 7 Service Pack 1 (32 or 64-bit) | 800MHz (1GHz recommended) | 1 GB (32-bit)<br>2 GB (64-bit) | |
| **Other Requirements** | | | |
| Web browser | Google Chrome™ - 81/83<br>Mozilla Firefox® - 75/76<br>Microsoft® Internet Explorer® 11.0<br>Microsoft Edge (Next) – 81/83<br>Microsoft Edge (Original) – Up to 44 | | |
| Display | Screen Resolution: 1024x768 or above | | |

**Table 4. Trend Micro Antivirus for Mac 2021 (v11)**

| Operating System | CPU | Memory | Disk Space |
|---|---|---|---|
| Mac OS® X version 10.15 or later (Catalina)<br>Mac OS® X version 10.14 or higher (Mojave) | Apple Macintosh computer with an Intel® Core™ Processor | 2 GB | 1.5 GB |
| **Other Requirements** | | | |
| Web Browser | Apple® Safari® 12.0 or later<br>Mozilla® Firefox® - the newest two versions<br>Google Chrome™ - the newest two versions | | |

**Table 5. Password Manager 5.0 (WIN, MAC) / 5.5 (Android, iOS)**

| Operating System (Windows) | CPU | Memory | Disk Space |
|---|---|---|---|
| Windows 10 (32bit and 64bit)<br>Windows 8.0, 8.1 (32bit and 64bit)<br>Windows 7 Service Pack 1 or above (32bit and 64bit) | 1 GHz or faster processor | 2 GB or more | 300+ MB |
| Web Browser | Microsoft Internet Explorer 11.0<br>Microsoft Edge (via Trend Micro Security for Edge) – the newest 2 versions<br>Mozilla Firefox – the newest 2 versions<br>Google Chrome – the newest 2 versions | | |
| **Operating System (Mac OS)** | **CPU** | **Memory** | **Disk Space** |
| Mac OS X 10.15 (Catalina)<br>Mac OS X 10.14 (Mojave) | Intel Core 2 Duo 2.0 GHz or faster processor | 2 GB or more | 300+ MB |
| Web Browser | Safari 12.0 or later<br>Mozilla Firefox – the newest 2 versions<br>Google Chrome – the newest 2 versions | | |
| **Mobile Operating System** | **Devices** | | |
| Android 5.0-10.0 | Android Smartphones App, Tablets App | | |
| iOS 11.0-13.0 | iOS iPhones, iPads, iPods | | |

**Table 6. Trend Micro Mobile Security 12.0 for Android**

| Requirements | Description |
|---|---|
| **Operating System** | **Android OS 4.1 or later** |

**Table 7. Mobile Security 9.0 for iOS**

| Requirements | Description |
|---|---|
| **Operating System** | **iOS 11.0 or later. 64-bit device required for latest version.** |

## Internet Connection, USB Installation

Trend Micro Security needs an Internet connection for you to register online, download installs and updates, obtain virus information, send email to support, and browse the Trend Micro web site. While online, Trend Micro Security also takes advantage of the Smart Protection Network's reputation systems in combination with Smart Scan to help obtain the reputation of files. See Section 6: Trend Micro Security and the Smart Protection Network for more details on the SPN and how users are still protected offline.

Note: Tend Micro may be transferred to another computer and installed from a USB thumb drive without any issues.

## Target Audience

The target audiences for the Trend Micro Security products are mainstream consumers and home/small offices with 10 users or less who need effective protection against viruses, spyware, and other malware that doesn't impact their system's memory consumption and other resources.

## Global Availability

September 9, 2020

## Contacting Trend Micro

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

## Consumer Support Line

(800) 864-6027
Monday - Friday, 5:00AM - 8:00PM Pacific

## Free Phone, Email and Chat support

Trend Micro offers free phone, email, and chat support. For more info, contact eSupport at: http://esupport.trendmicro.com/support/consumer/consumerhome.do?locale=en_US

You can also contact the Trend Community at: http://community.trendmicro.com/

## Premium Support Services

Trend Micro provides users with Premium Support Services for a wide variety of technical issues including installation, virus and spyware removal, PC Tune-ups, etc. These services are offered as Ultimate or Premium bundles or as ad-hoc services. For more information, select **Premium Services** in the **Trend Micro Security Console > ID** drop-down menu, or go directly to Premium Support Services.

# Chapter 2: Installing and Activating Trend Micro Security

Trend Micro™ Security has separate installs for each version of the product:

- Trend Micro™ Antivirus+ Security
- Trend Micro™ Internet Security
- Trend Micro™ Maximum Security
- Trend Micro™ Antivirus for Mac®

(See our separate Product Guide for instructions to install and use Trend Micro™ Antivirus for Mac®.)

In the following example we install Trend Micro Maximum Security on Microsoft Windows 10, but each version of Trend Micro Security has a nearly identical installation and activation process for the various versions of Windows.

## Install Trend Micro Security

**To install Trend Micro Security on Windows 10 using a Download:**

1. Go to https://www.trendmicro.com/en_us/forHome.html to download Trend Micro Security. The main page **For Home** appears.

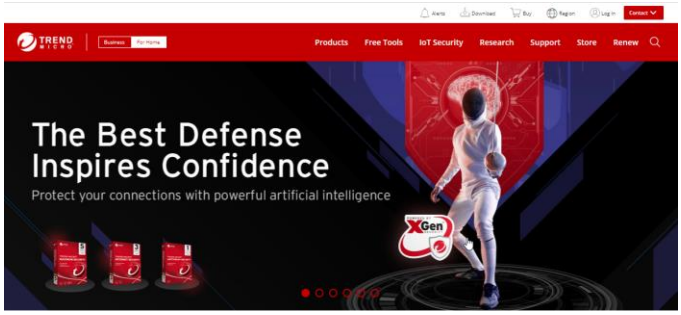



**Figure 1. Trend Micro - For Home**

**Paid Version:**

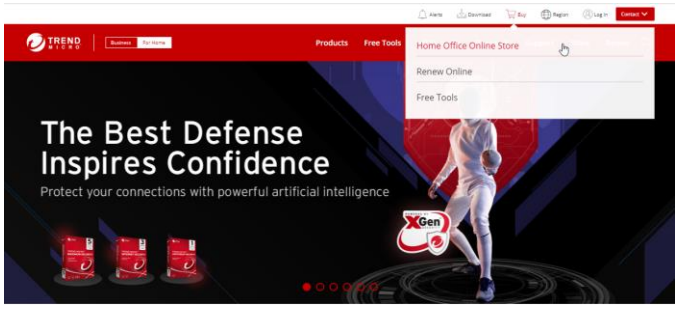



**Figure 2. Home Office Online Store**

1. If you want to buy Trend Micro Security, click **Buy > Home Office Online Store** in the upper right-hand corner of the **For Home** webpage. The **Home & Home Office Store** appears.

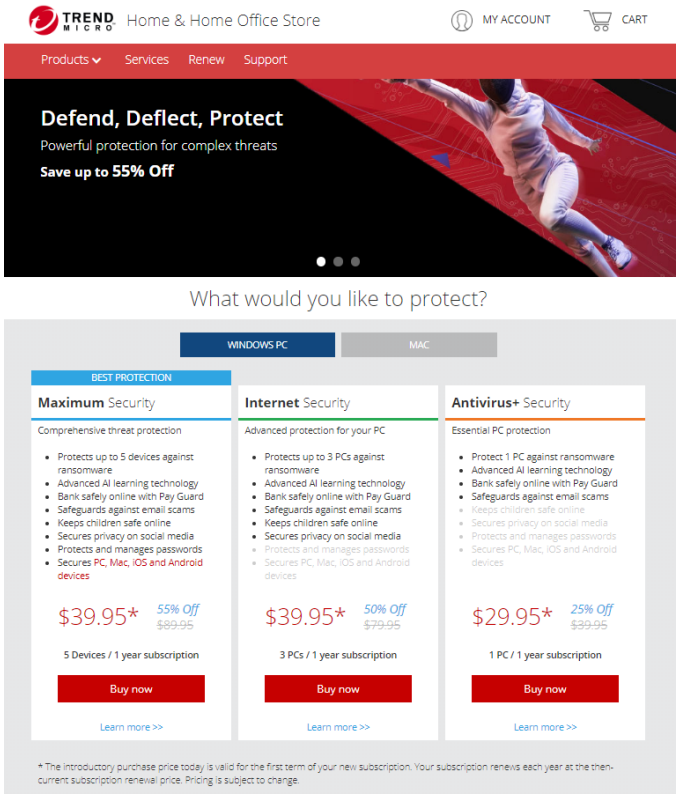



**Figure 3. Buy Now**

2. Select an edition that works for you and click **Buy Now,** then follow the directions to complete your purchase.

**Trial Version:**

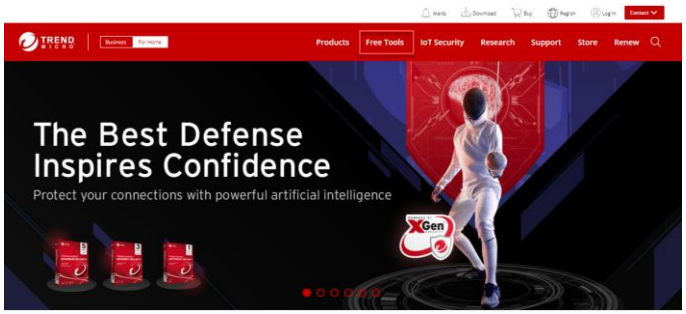



**Figure 4. Free Tools (1)**

1. If you want to install a **Trial** version, click the **Free Tools** menu item in the **For Home** webpage. The **Free Tools** page appears.

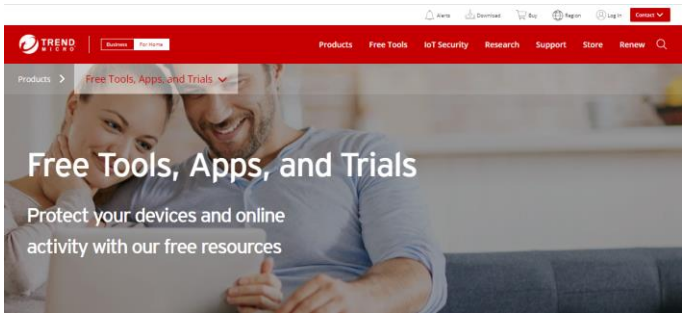



**Figure 5. Free Tools (2)**

2. Scroll down to the edition of Trend Micro Security you wish to download and click the **Download** icon.

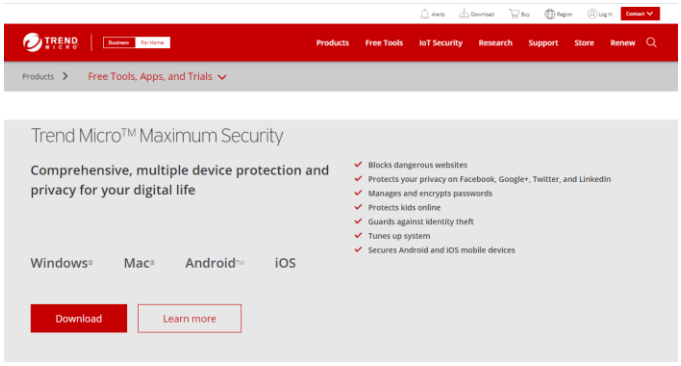



**Figure 6. Trial Download Button**

3. A popup window appears asking “Why try when you can buy?”

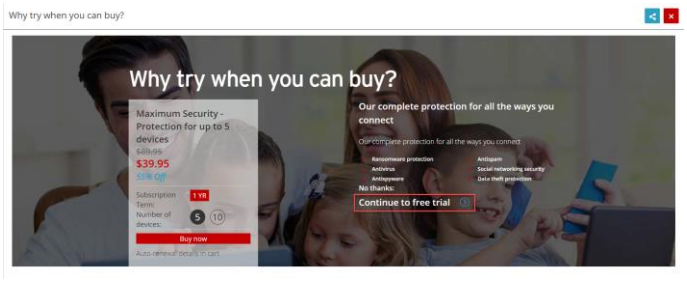



**Figure 7. Continue to Free Trial**

4. Click **Continue to Free Trial.** You're taken to the eSupport webpage, where you can download the **Trial**.

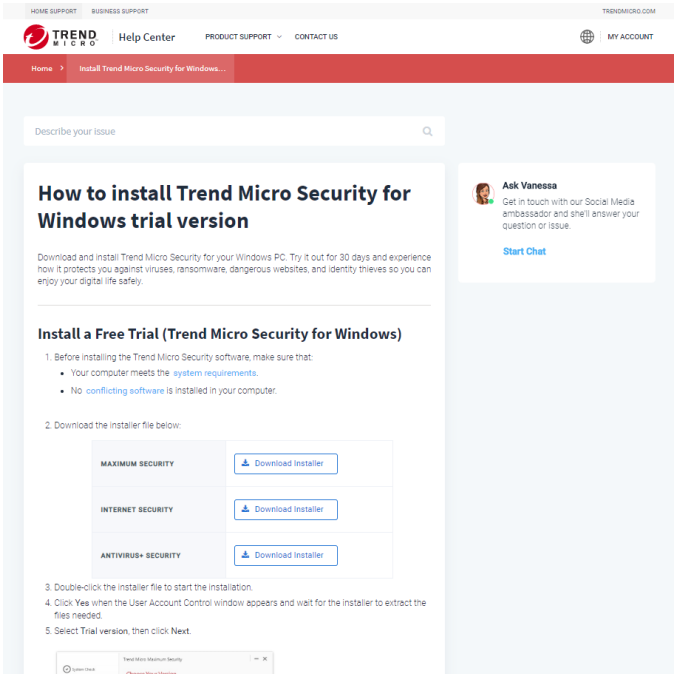



**Figure 8. Install Trial Version**

5. In this example, click the **Download Installer** button for Maximum Security. A **Save As** dialog window appears.

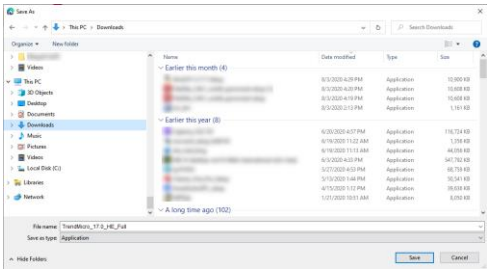


**Figure 9. Save As**

6. Navigate to the **Downloads** folder where you'll put the downloader and click **Save**. The **Downloader** execution file downloads and displays at the bottom of your browser (Edge sample below).

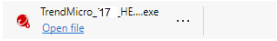



**Figure 10. Downloader Exe (Edge)**

7. Click **Open File**. Trend Micro Security finishes the file download and a Windows **User Account Control** pop-up dialog appears, asking if you want to allow the app to make changes to your computer.

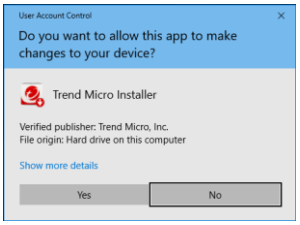



**Figure 11. User Account Control**

8. Click **Yes**. The installation begins, extracts the installer files, and gives you a progress screen.

**Figure 12. Unpacking Files**

9. Trend Micro Security will then do a **System Check**, to see if your computer meets the minimum system requirements and will conduct a quick malware scan.

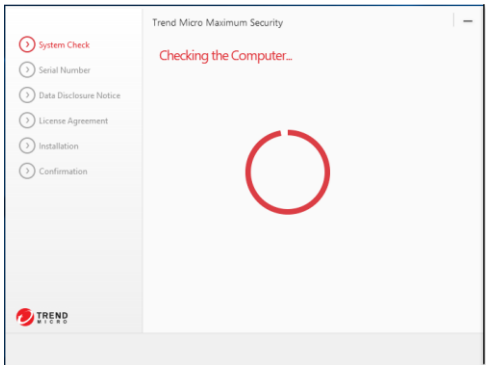



**Figure 13. Checking the Computer**

10. When the process completes, a **Serial Number** screen appears, asking you to **Choose Your Version.**

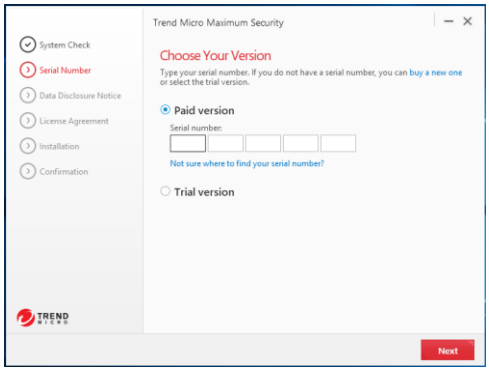



**Figure 14. Choose Your Version > Paid**

11. If you're installing a **Paid** version, enter the **serial number** provided by Trend Micro in your retail box or confirmation email, then click **Next**.

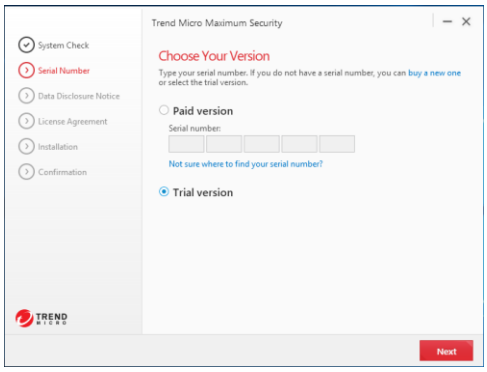



**Figure 15. Choose Your Version > Trial**

12. If you're installing a **Trial** version, click the **Trial** version button, then click **Next**.
13. In each case, the **Privacy and Personal Data Collection Disclosure** appears.

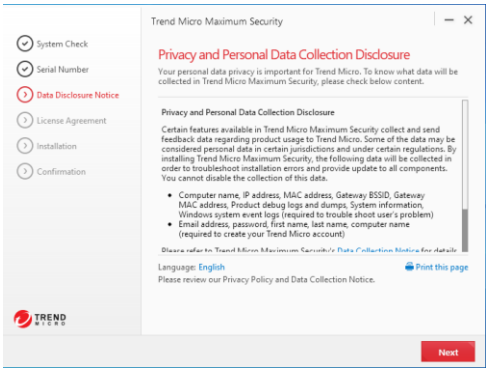



**Figure 16. Privacy and Personal Data Collection Disclosure**

14. Read the **Privacy and Personal Data Collection Disclosure** to know what kind of feedback and detection data will be collected by Trend Micro, then click **Next**. The **License Agreement** appears.

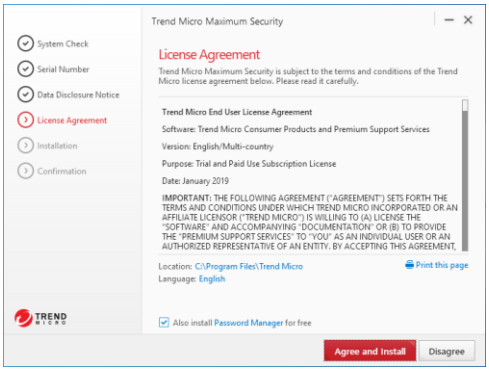



**Figure 17. License Agreement**

15. Trend Micro Security chooses a default location for the installation. You can change this by clicking the **Location** link and browsing to another location. (Trend Micro recommends you use the default.)
16. If you wish, click the **Language** link to stop the software from automatically adjusting to the language of your operating system, then pick the language you want the software to display.
17. Note too that **Password Manager** is installed automatically with Trend Micro Maximum Security. Uncheck the checkbox if you don't wish to also install **Password Manager.**
18. Read the **License Agreement** using the scrollbar. If you agree with the **License Agreement**, click **Agree and Install**. (Click **Print this page** to print it out.)
19. Trend Micro Security begins the installation. This takes a few minutes. A progress indicator indicates the stages and progress of the install.

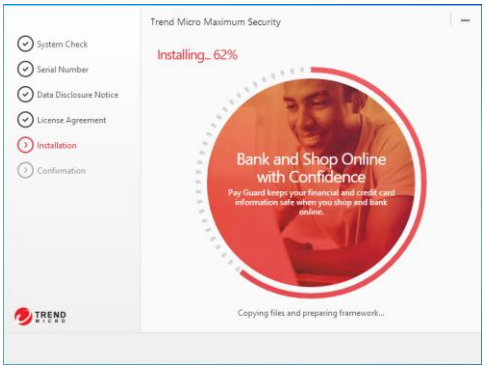



**Figure 18. Progress Indicator**

### Trial Version

1. When the installation is complete, if you've installed a **Trial** version, a screen appears saying **Activate Your Protection.**

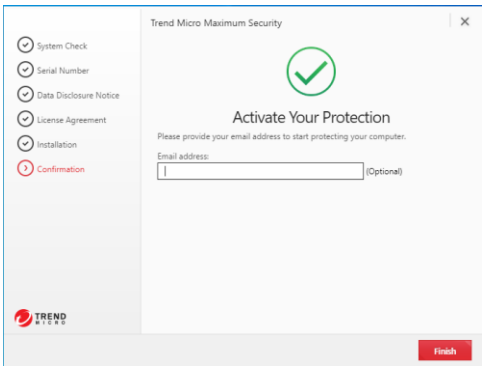



**Figure 19. Activate Your Protection (Trial Version)**

2. Please provide your email address to start protecting your computer (Optional) and click **Finish**. This completes your installation.

### Paid Version

1. If you've installed a **Paid** version, you have two options for the email address:
   - **Use an existing Trend Micro Account.** Provide the email address for this account.
   - **Create a new Trend Micro Account.** Provide a preferred email address

**Use an existing Trend Micro account:**

2. If you have activated Trend Micro software before, simply enter the email address you used to create your account when you purchased the product and click **Next**. The **Sign In** screen appears.

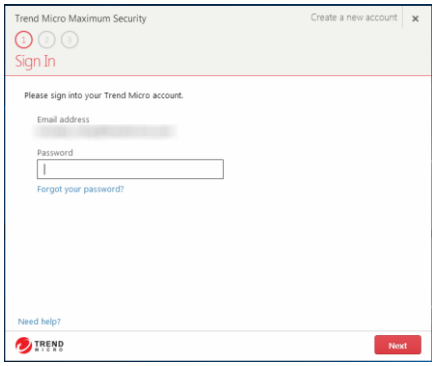



**Figure 20. Sign In**

3. Enter the **Password** for your Trend Micro account and click **Next**. A screen appears for you to name the computer.

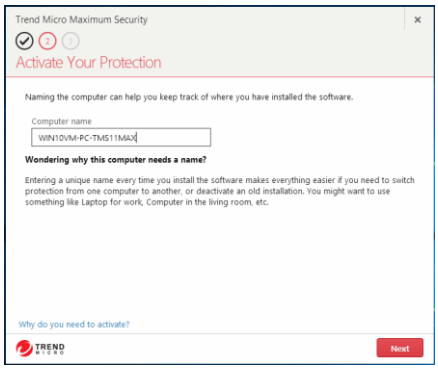



**Figure 21. Computer Name**

4. To help track your subscription, use the name of your computer as it is automatically entered, or enter a "friendlier" name to best identify it and click **Next**.

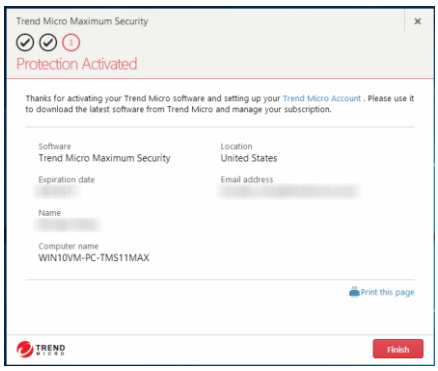



**Figure 22. Protection Activated**

5. Your **Protection is Activated** and the installation is complete. Click **Finish** to close the dialog.

**Create a new Trend Micro account:**

1. If you have **not** activated Trend Micro software before, enter the preferred email address you'll use for your purchase activation and click **Next**. A screen appears, asking you to **Enter Account Information.**

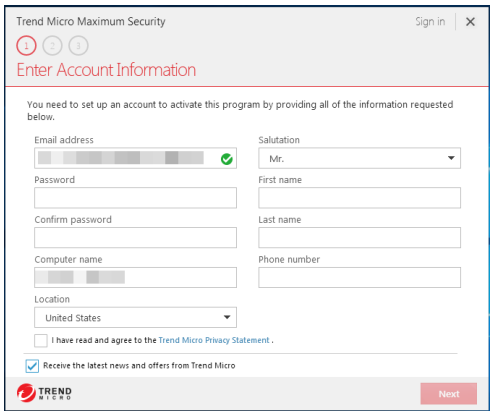



**Figure 23. Enter Account Information**

2. Enter your account information. For the password, use only simple letters and numbers, but not less than 8 characters. For the computer name, use the name of your computer that's automatically entered, or enter a new name to identify it.

3. Read the **Trend Micro Privacy Statement**. If you agree, check **I have read and agree to the Trend Micro Privacy Statement.**

4. You may retain or remove the check to **Receive the latest news and offers from Trend Micro** and click **Next**. A screen appears for you to **Check What You Entered.**

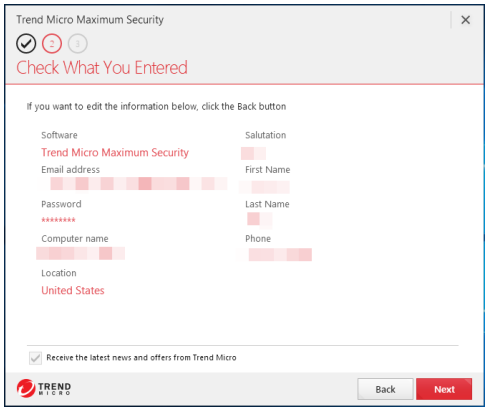



**Figure 24. Check What You Entered**

5. If your entries are accurate, click **Next**. A dialog indicates **Protection Activated.** You may print this page.

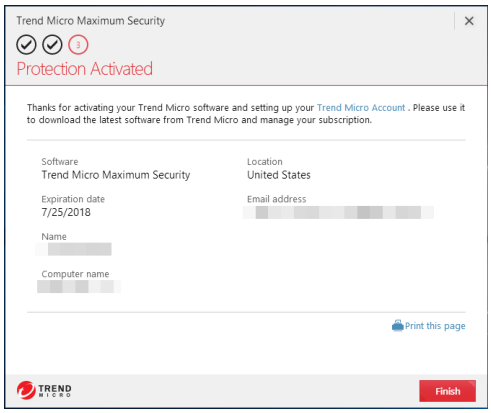



**Figure 25. Protection Activated**

6. Click **Finish**.

7. In each purchased case, once your protection is activated, Trend Micro Security pops up a window, asking if you wish to receive monthly email reports.

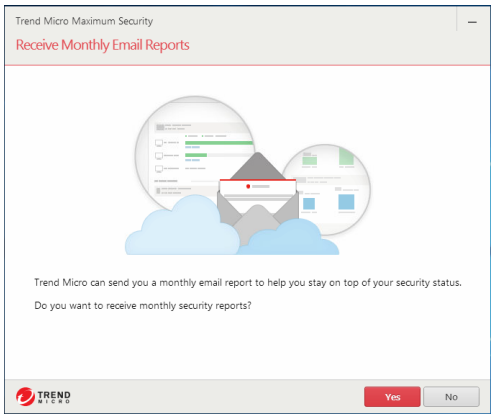



**Figure 26. Receive Monthly Email Reports**

8. Click **Yes** if you wish to receive monthly security reports. A window with your **Subscription Information** appears.

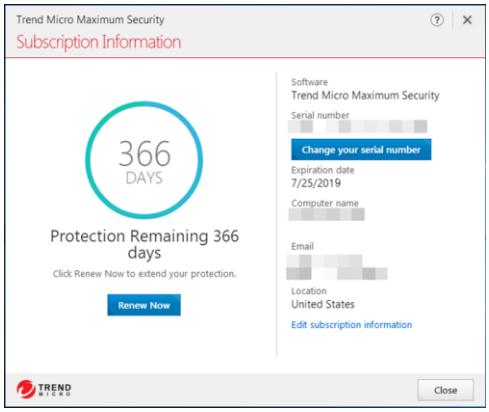



**Figure 27. Subscription Information**

9. Click **Close** to close the **Subscription Information** window.
10. A popup appears saying **Your PC is Now Protected.**

**Figure 28. Your PC is Now Protected**

11. Click **OK** to finish the installation, or **Explore More Features** to do so.

- If you choose the first option, you'll be prompted to **Protect Yourself from Ransomware** by setting up **Folder Shield** and to **Secure and Enhance Your Mobile Life** by installing **Trend Micro Mobile Security** on your mobile devices.

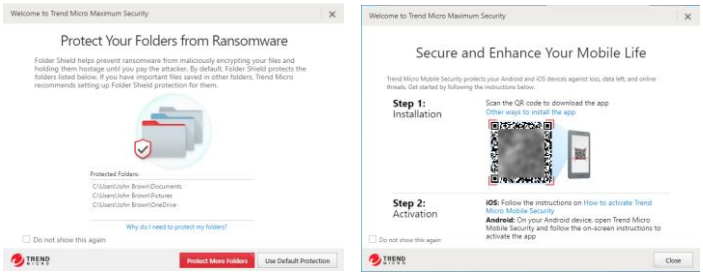



**Figure 29. Protect from Ransomware - Enhance Your Mobile Life**

- If you choose the second option, you're given a questionnaire and wizard to help you get started using **Trend Micro Security.** See the sections following for more details.

12. For now, close the **Welcome** window to complete the installation.

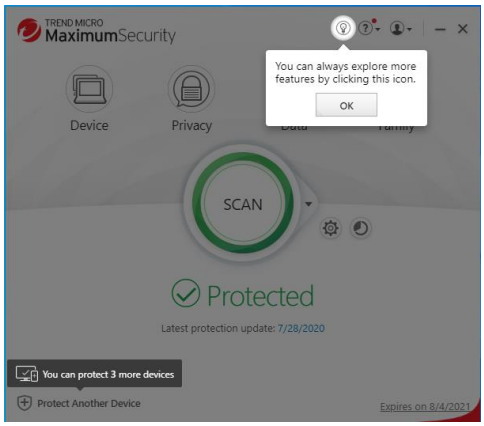



**Figure 30. Reminder Popups**

13. The **Trend Micro Security Console** appears, with a popup indicating that you can always explore more features by clicking this icon (the **Lightbulb** icon), which will display the features option window you've just seen. Another popup indicates how many more devices you can protect with your subscription (for example, three or four more devices out of your 5-seat subscription).

14. Click **OK** to close the popups. The **Trend Micro Security Console** shows that you are **Protected**.

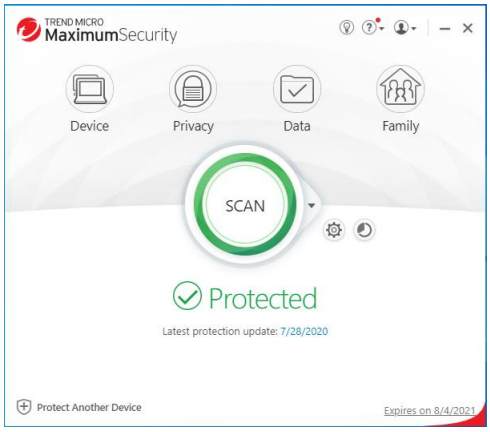



**Figure 31. Trend Micro Maximum Security - Protected**

15. Click the **Close (X)** icon to close the window. Trend Micro Security is now protecting your computer.

# Explore More Features – Questionnaire and Wizard

Trend Micro Security provides a questionnaire and wizard to help you get started with key features of the software.

**Figure 32. Explore More Features**

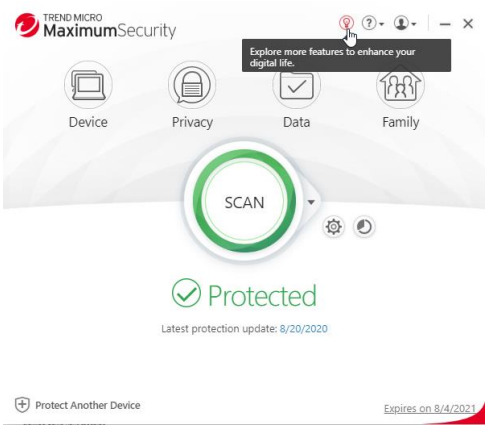



**Figure 33. Trend Micro Security Console**

1. After installation, if you choose the second option **Explore More Features** in the **Welcome** screen, or click the **Lightbulb** icon at any time in the **Main Console**, a screen appears prompting you to **Find useful features by answering a few questions.**

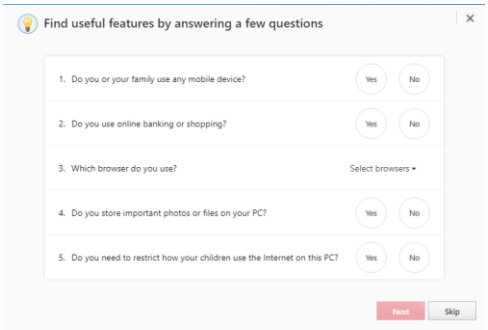



**Figure 34. Explore More Features**

2. Click all the **Yes** or **No** buttons that apply to your use case.

3. Use the drop-down menu to **Select Browsers.** A popup appears, letting you select the browsers you use.

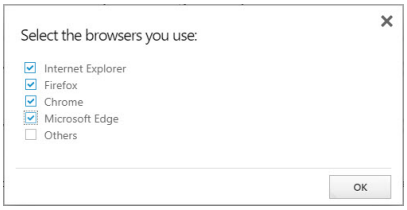



**Figure 35. Select the Browsers You Use**

4. Click the checkbox to select the browsers you use, then click **Next**. A screen appears, showing buttons to explore and activate some features that you might find useful.

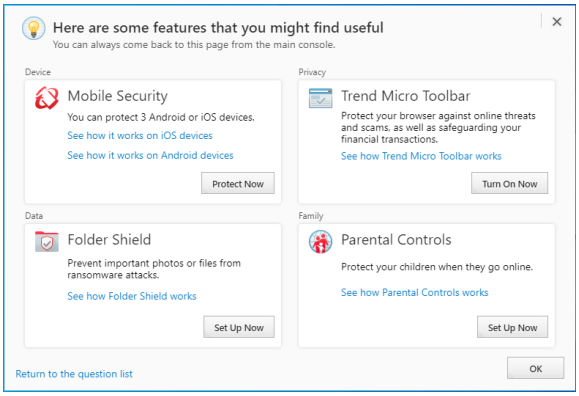



**Figure 36. Features You Might Find Useful**

5. In the screen shown, you have four options:

- **Mobile Security.** Click **Protect Now** to protect your Android or iOS devices. A screen appears with a QR Code you can scan to install Trend Micro Mobile Security on your Android or iOS device.

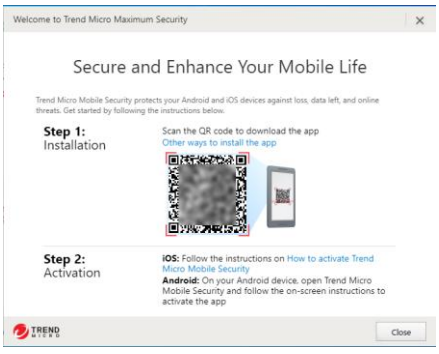



**Figure 37. Install Mobile Security**

- **Folder Shield.** Click **Set Up Now** to select the **Folders** (and their enclosed Files) you wish to protect from ransomware attacks. A screen appears for you to **Protect More Folders** or **Use Default Protection.**

**Figure 38. Protect Your Folders from Ransomware**

- **Trend Micro Toolbar.** Click **Turn On Now** to turn on the **Trend Micro Toolbar** in your chosen browsers. A screen appears for you to **Install** or **Turn On** the Toolbar.

**Figure 39. Install Trend Micro Toolbar**

- **Parental Controls.** (For Internet Security and Maximum Security.) Click **Set Up Now** to set up **Parental Controls** to protect your children when they go online. A screen appears for you to **Select a Password** to protect your **Parental Controls** settings, so they can't be changed without your password. You then complete the process for tailoring protection for the specific child, with age-appropriate settings. See the **Family: Parental Controls** section in this guide to learn more.

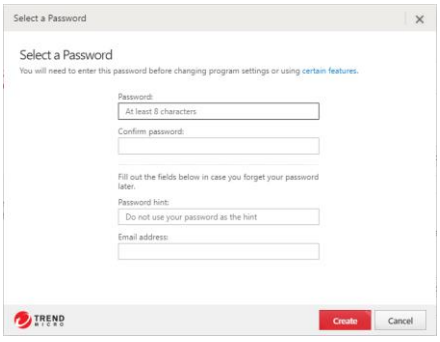



**Figure 40. Select a Password - Begin to Set Up Parental Controls**

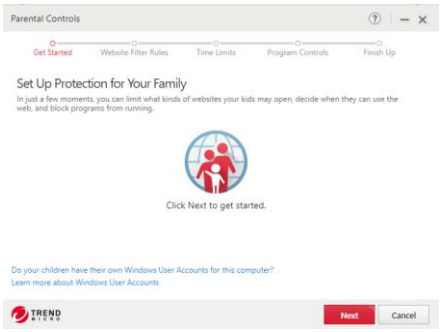



**Figure 41. Set Up Protection for Your Family**

# Protect Another Device

Subscriptions to Trend Micro™ Antivirus+, Internet Security, and Maximum Security variously let you protect other PCs and Macs, as well as Android and iOS mobile devices.

- Trend Micro Antivirus+: 1 PC, though you may switch your protection to another PC
- Trend Micro Security Internet Security: up to 3 PCs and Macs
- Trend Micro Security Maximum Security: from 5 to 10 devices, including PC, Mac, Android and iOS Mobile devices

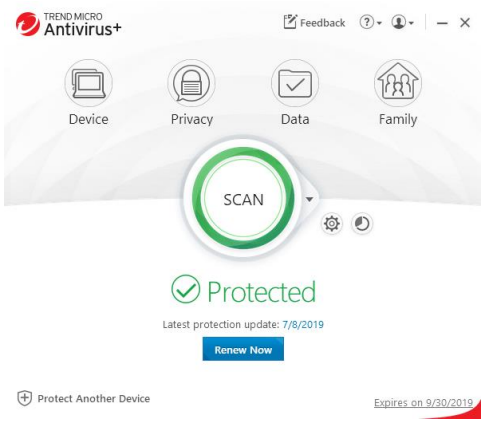



**Figure 42. Protect Another Device**

1. To get started with your protection for another device, launch Trend Micro Security.
2. Click **Protect Another device.** The **Protect Another Device** screen appears. The range of options depends on the edition of Trend Micro Security you have purchased.

**Note:** **A subscription to Trend Micro Antivirus+ allows you to protect only one device. To transfer this subscription to another device you need to log into your My Account page, download the installer on the second device, and install it. Once you register the application, you'll be given the option to disable Trend Micro Antivirus+ on the first device so you can activate it on the second.**

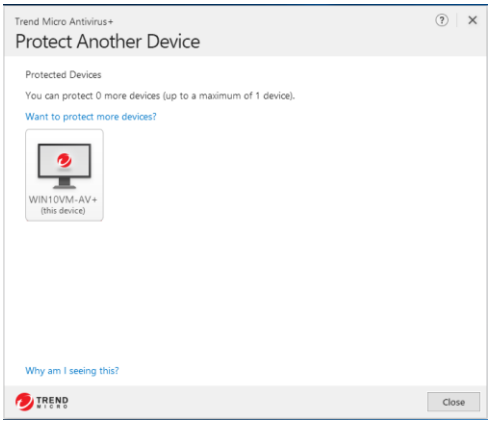



**Figure 43. Antivirus+ > Protect Another Device**

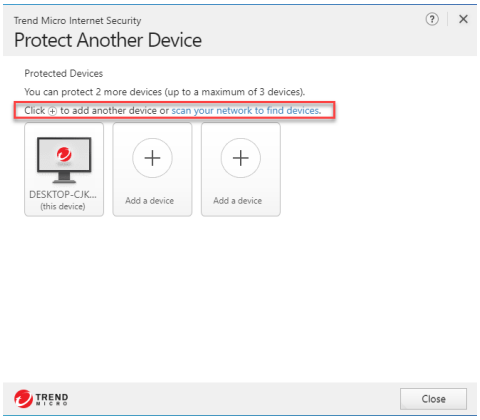



**Figure 44. Internet Security > Protect Another Device**

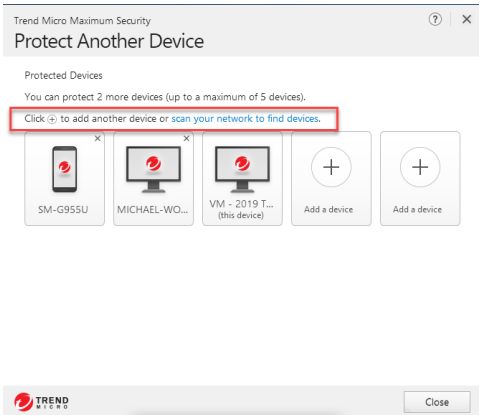



**Figure 45. Maximum Security > Protect Another Device**

3. With Trend Micro Internet or Maximum Security, you can click the link **scan your network to find devices** on your network. A popup appears asking “Do you want Trend

Micro Internet/Maximum Security to scan your home network (LAN) to find connected devices?”

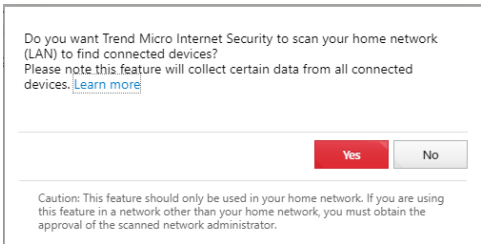



**Figure 46. Scan Prompt**

4. Click **Yes** to scan your network. The scan begins.

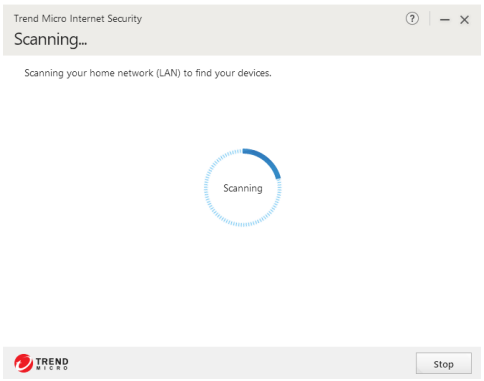



**Figure 47. Scanning for Other Devices**

5. When the scan is complete, a **Scan Results** screen appears.

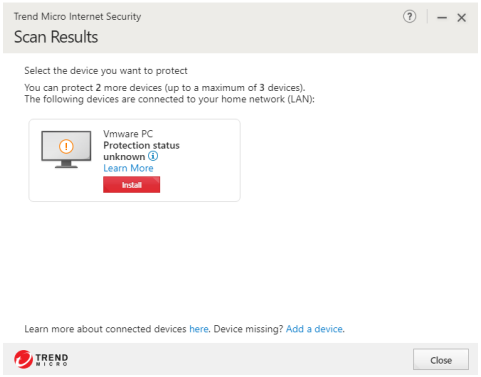



**Figure 48. Devices Found > Install**

6. If the **Scan Results** finds other devices to protect, it provides an **Install** button to install protection on that device.

7. Tap **Install** to install Trend Micro Security/Mobile Security on that device. A screen appears, with options for downloading and installing it.

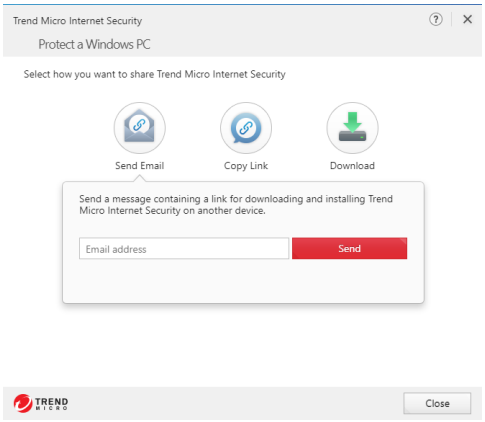



**Figure 49. Protect a Windows PC**

8. If it finds no devices, the screen says **No Devices Found.**

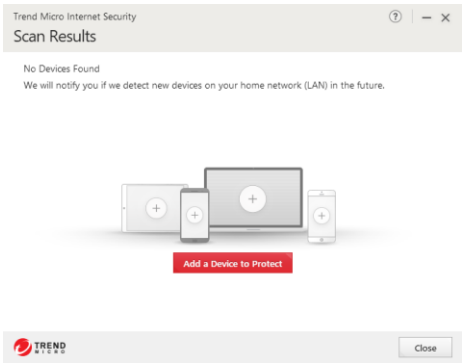



**Figure 50. No Devices Found > Add a Device to Protect**

9. If you know that your family has other devices currently not on the network, you can still tap **Add a Device to Protect.** The **Protect Another Device screen** appears.

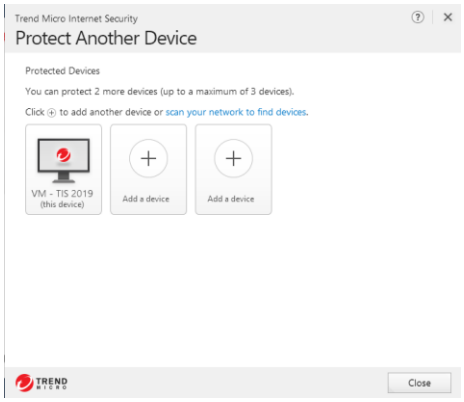



**Figure 51. Protect Another Device**

10. For Trend Micro Internet and Maximum Security, click an icon to **Add a device.** A popup appears, letting you choose the platform you would like to share protection with.

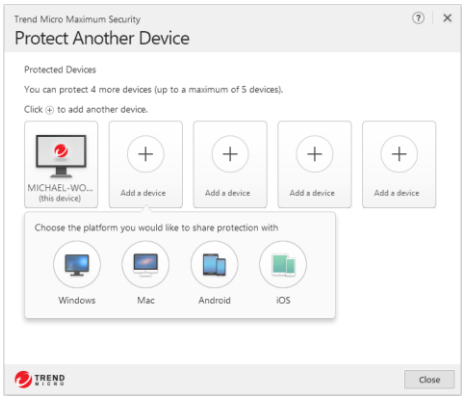



**Figure 52. Add a Device Popup**

11. Click the icon for your chosen platform. A screen appears, providing email, copy link, and download options for getting the software.

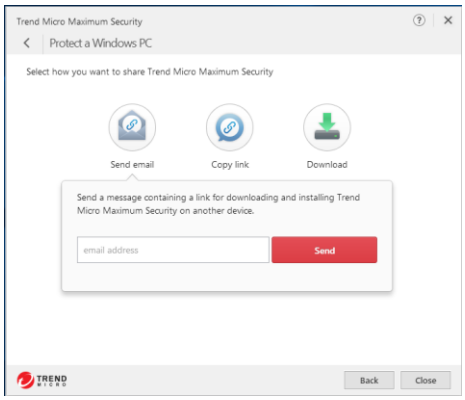



**Figure 53. Send Email**

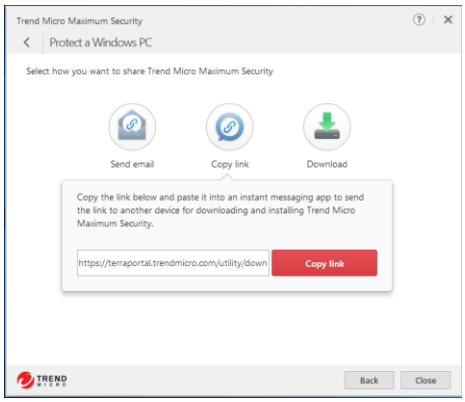



**Figure 54. Copy Link**

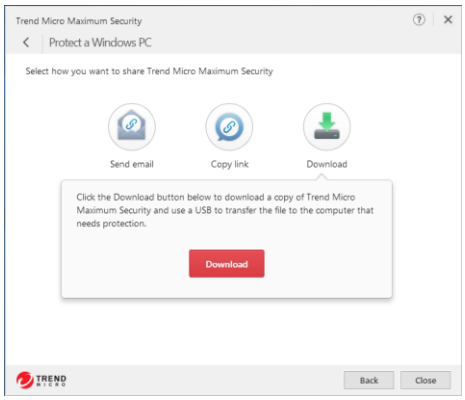



**Figure 55. Download**

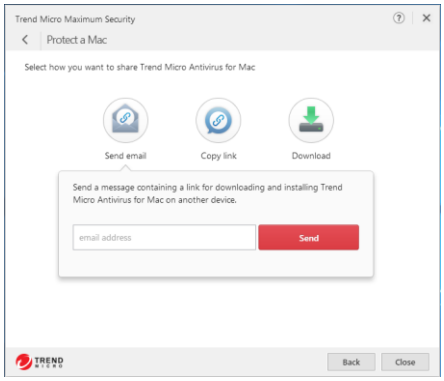



**Figure 56. Protect a Mac**

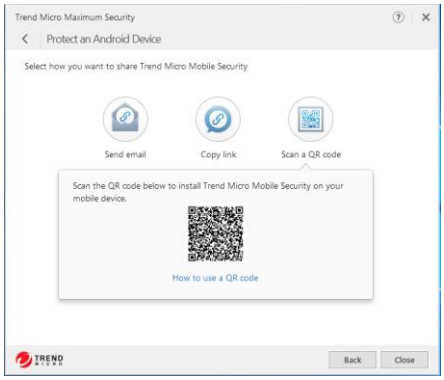



**Figure 57. Protect an Android Device**

12. For PC or Mac protection, pick how you want to get the application: Email, Link, or Download. If you download the installer to your active computer, you may use a USB thumb drive to physically take the file to the other computer.
13. For Android or iOS protection, pick how you want to get the app: Email, Link, or QR Code, (for Google Play™, Trend Micro™, Amazon Appstore™, or Apple App Store™).
14. To install, follow the instructions on the page, store, or email.

# Set Up Folder Shield

1. Trend Micro strongly urges you to set up **Folder Shield** right after you've installed Trend Micro Security, to protect yourself from ransomware. The default setting is quick and easy to enable.

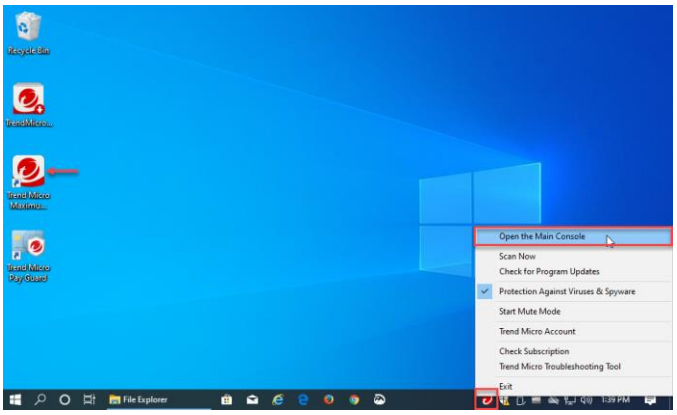



**Figure 58. Open the Main Console**

2. Click **Open the Main Console** in the Trend Micro Security menu in the **System Tray**, or double-click the **Trend Micro Security** shortcut on the desktop. The **Trend Micro Security Console** appears, with the **Welcome to Trend Micro Security** screen in front of it.

**Figure 59. Protect Your Folders from Ransomware**

3. By default, Folder Shield shows the Protected Folders it has selected for you. You may **Use Default Protection**, or click **Protect More Folders.**

4. In this example, we'll click **Protect More Folders.** The **Manage Folders** window appears, letting you choose the folders you wish to protect.

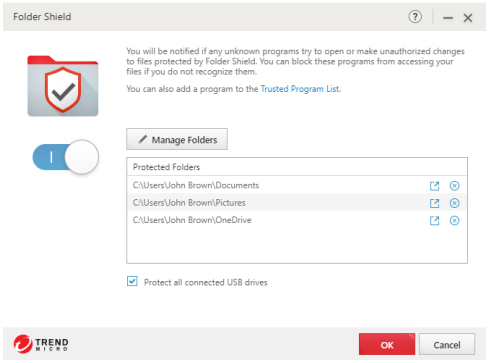



**Figure 60. Manage Folders**

5. The default **Protected Folders** are shown in the window, along with protection for all connected USB drives by default. Click **Manage Folders** if you wish to add folders to protect. A window appears, allowing you to **Choose Folders to Protect.**

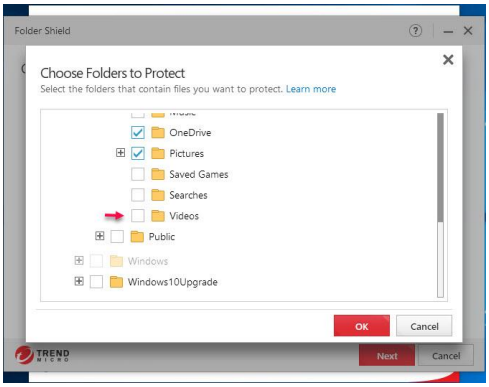



**Figure 61. Add Videos**

6. In this example, we'll scroll down and add **Videos** to the folders protected by **Folder Shield** by checking its checkbox and clicking **OK**. The **Videos** folder now appears in the **Protected Folders** list.

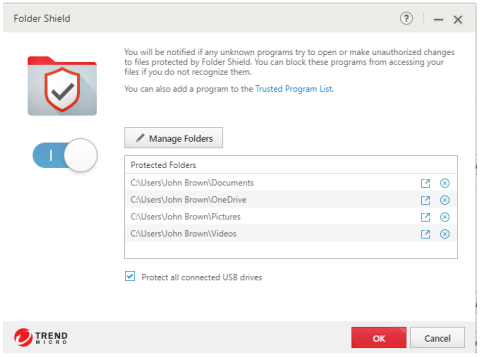



**Figure 62. Videos Added to Protected Folders**

7. Click **Ok**. The **Manage Folders** window indicates **Folder Shield Setup Complete.**

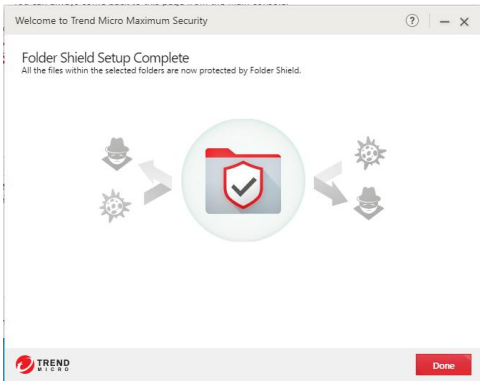



**Figure 63. Folder Shield Setup Complete**

8. Click **Done** to close the window. **Folder Shield** is now activated and your protected folders are now shielded from malicious changes by any programs that are not in Trend Micro's list of known good programs, such as ransomware.

9. At any time, you can return to the **Manager Folders** window to add more folders to protect. See the **Data: Folder Shield** section for more details.

## Install Trend Micro Security for Microsoft Edge

Microsoft Edge is now the default browser in Microsoft Windows 10. Once you've installed Trend Micro Security, you should install the **Trend Micro Security for Microsoft Edge** extension to improve your browsing protection. It provides **Web Threat Protection, Fraud Buster, Ad Block, Privacy Scanner, and Pay Guard**, and works in conjunction with **Password Manager** in the following configurations:

- **Trend Micro Antivirus+** and **Internet Security**: Password Manager supports 5 pass cards.
- **Maximum Security**: Password Manager supports unlimited pass cards.

**Note:** **Trend Micro Security for Microsoft Edge provides direct access to the Trend Micro Password Manager Web Management Console. For password capture and replay, however, you still need to separately install Password Manager when using Trend Micro Antivirus+ or Internet Security. When you install Trend Micro Maximum Security, Password Manager is automatically installed at the same time, unless you opt out.**

1. When you launch **Microsoft Edge**, after a time you will be prompted to install **Trend Micro Security for Microsoft Edge**, to **Safeguard Your Browser**.

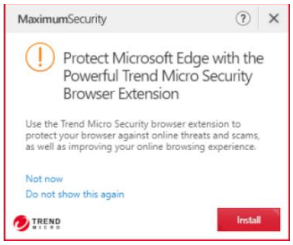



**Figure 64. Protect Microsoft Edge**

1. Click **Install** in the popup. You may also obtain the extension by clicking **Trend Micro Security for Microsoft Edge.** Both will launch the **Edge Add-ons Store** and take you to directly to the **Trend Micro Security** page**.**

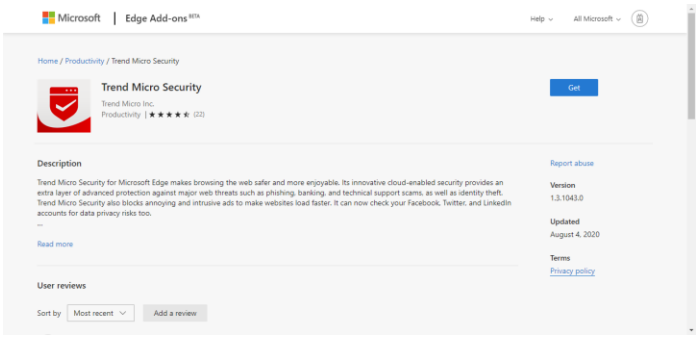



**Figure 65. Edge Add-ons - Trend Micro Security for Edge**

2. Click **Get** to get the app. A popup appears to add the extension.

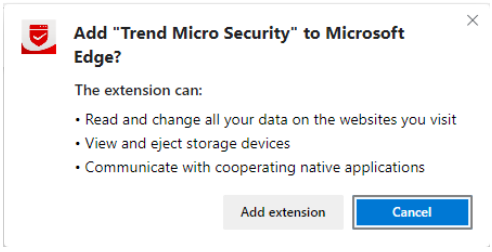



**Figure 66. Launch Trend Micro Security**

3. Click **Add Extension**. The **Trend Micro Security** extension installs. A page appears to **Start Your Protection.**

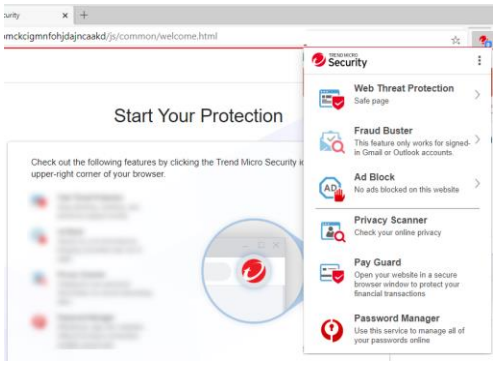



**Figure 67. Start Your Protection**

4. Click the **Trend Micro Security** icon in the main browser menu. The drop-down menu shows the features provided:

   - **Web Threat Protection.** Protects you from Web threats when you search or browse the Web.
   - **Fraud Buster.** Protects you against fraudulent emails when you're signed into Gmail or Outlook webmail.
   - **Ad Block.** Blocks ads from displaying on websites.
   - **Privacy Scanner.** Check your privacy settings in Facebook, Twitter, and Linked In. Also enhances your privacy when using Internet Explorer, Google Chrome, and Firefox.
   - **Pay Guard.** Protects you from malicious websites and scripts when buying or banking online.
   - **Password Manager.** Provides access to the Password Manager Web Management Console. (Capture/replay of passwords requires a separate Password Manager install.)

## Web Threat Protection

Web Threat Protection is the first protection feature provided in Trend Micro Security for Edge.

**To use Web Threat Protection:**

1. While searching or browsing the web, **Web Threat Protection** will block you if you attempt to go to a dangerous page,

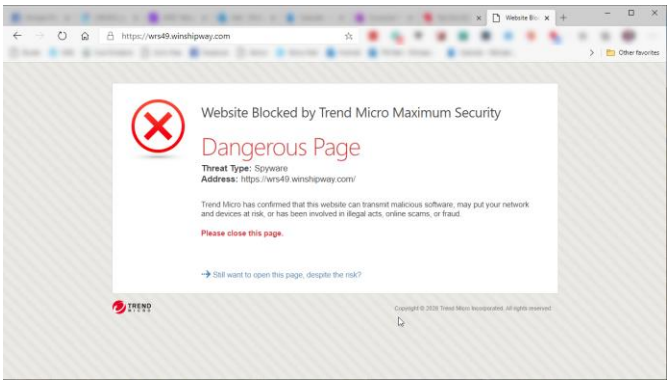



**Figure 68. Web Threat Protection Block**

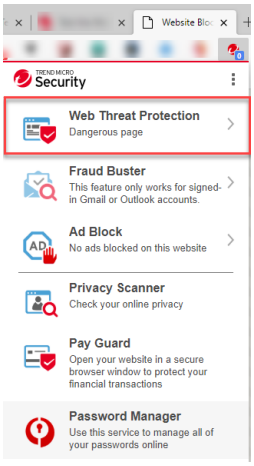



**Figure 69. Web Threat Protection**

2. Click the **Web Threat Protection** panel in the drop-down menu to review the **Trend Micro Security 30-day report** of pages scanned and blocked.

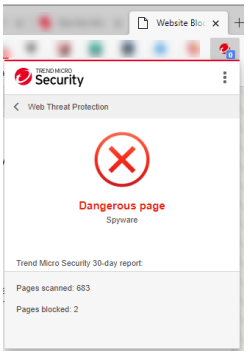



**Figure 70. Trend Micro Security 30-day Report**

## Fraud Buster for Gmail and Outlook Webmail

More and more scam emails these days may contain no obvious malicious URLs or attachments but can nonetheless be a threat, using social engineering to snare the unsuspecting user. However, such emails can't be detected by traditional email security technology.

**Fraud Buster** is designed to deal with this type of scam email, using artificial intelligence (AI) technology to identify the topic and to understand the intention of the scam. As part of TMS for Edge (and Trend Micro Toolbar), **Fraud Buster** protects Gmail and Outlook webmail in Microsoft Edge, Internet Explorer, Chrome, and Firefox. The example below uses **TMS for Edge** to show the setup.

**To enable Fraud Buster:**

1. **Fraud Buster** requires first that you log into your Gmail or Outlook webmail account.

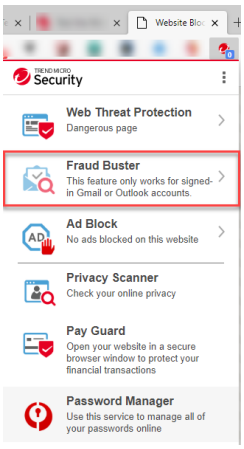



**Figure 71. Log Into Gmail or Outlook to Enable Fraud Buster**

2. For example, log into your Gmail account.

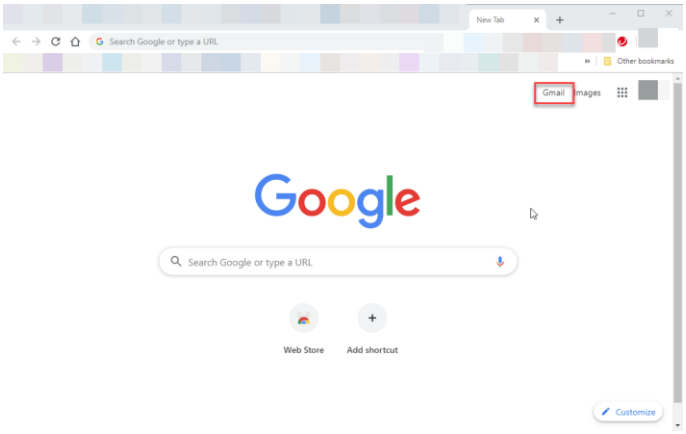



**Figure 72. Gmail Button in Chrome**

3. Then, on the Google home page, click **Gmail** to open your **Gmail** webmail. A popup appears for you to **Protect Your Webmail.**

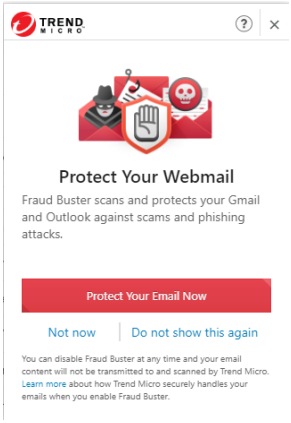



**Figure 73. Protect Your Webmail**

4. Click **Protect Your Email Now.** Another popup appears, describing how **Fraud Buster** protects your Gmail and Outlook.com against scams and phishing attacks by sending your email content to Trend Micro to scan.

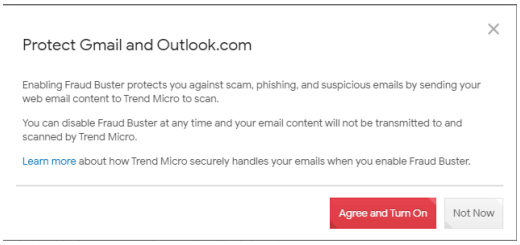



**Figure 74. Protect Gmail and Outlook.com**

5. If you agree to it, click **Agree and Turn On.**

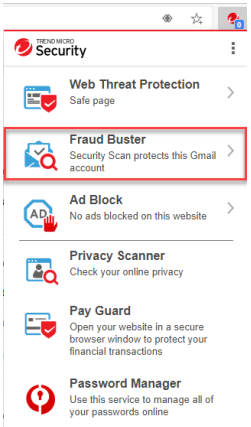



**Figure 75. Gmail Protected by Fraud Buster | Active in TMS for Edge**

6. **Fraud Buster** is now enabled and you can see it active in **TMS for Edge**.

7. Your Gmail (or Outlook.com) webmail will now be scanned for potential scams and you'll be alerted with a warning popup when you open a scam email, telling you to not follow any instructions contained in the email.

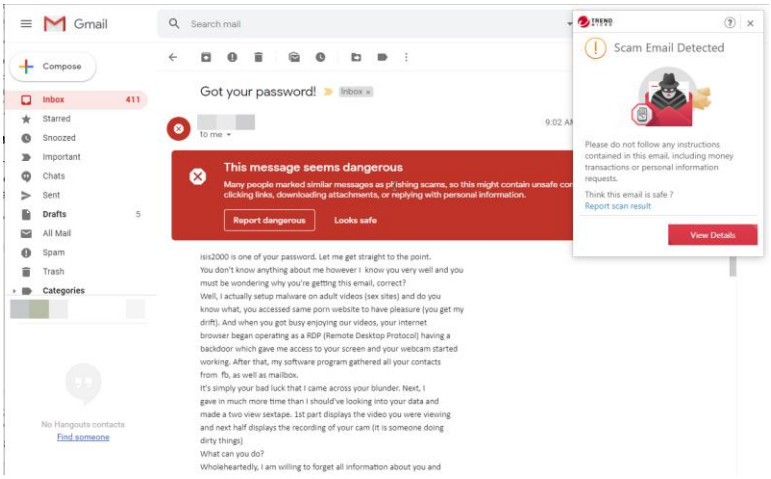



**Figure 76. Scam Email Detected**

8. You can click **Report Dangerous** to report the scam webmail or **Looks Safe** to bypass the warning (not recommended). In this example, click **View Details** in the popup warning to get more details about the scam.

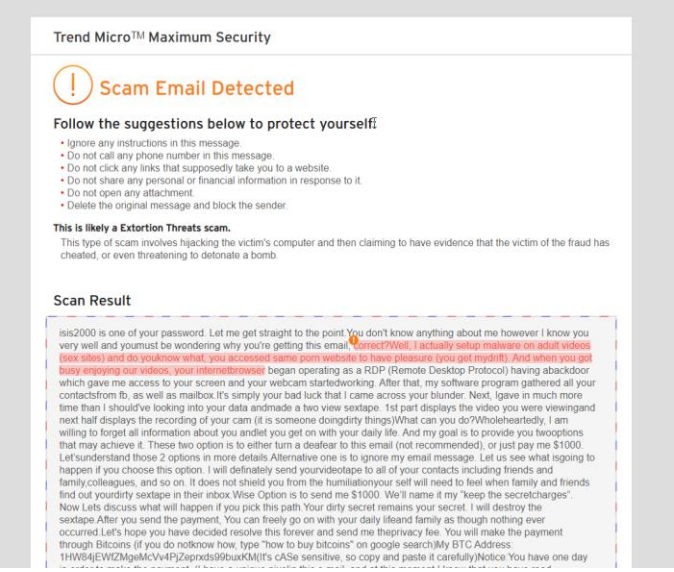



**Figure 77. Scam Email Detected: Details**

9. Follow Trend Micro's instructions to better protect yourself from scams; or contact Trend Micro to get more support. When done, close the **Details** window and scam email, then delete the scam email from your inbox.

## Ad Block

**Ad Block** blocks ads from displaying in Microsoft Edge. With **Ad Block** active, if you go to a page with advertising, the ads will be blocked. In the screen shown below, 14 ads were blocked.

### To Stop/Resume Ad Block

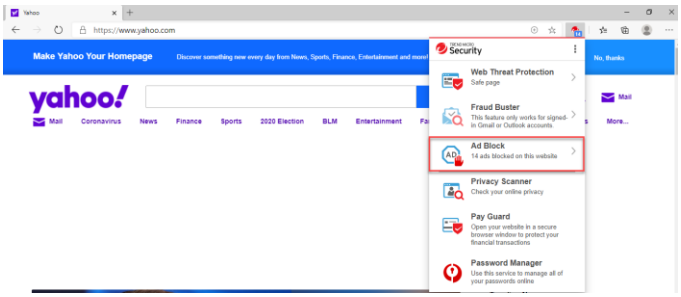



**Figure 78. 14 Ads Blocked**

1. Click **Ad Block** in the drop-down menu. The drop-down menu pages leftward to let you **Stop** or **Resume Ad Block** by clicking the **Stop/Resume Add Block** button. You can also use the slider to turn off the feature.

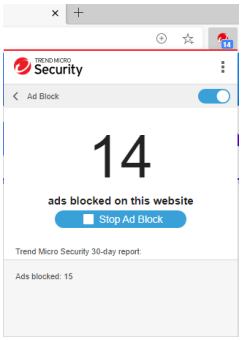



**Figure 79. Stop Ad Block | Turn Off Trend Micro Security Slider**

## Privacy Scanner

**Privacy Scanner** lets you check your privacy settings in Facebook, Twitter, or Linked In. You can additionally enhance your privacy in Internet Explorer, Google Chrome, and Mozilla Firefox.

**To use Privacy Scanner:**

1. Click **Privacy Scanner** in the drop-down menu to check your privacy setting in **Facebook, Twitter, or Linked In.**

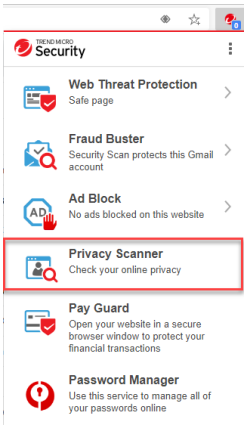



**Figure 80. Privacy Scanner**

2. The **Privacy Scanner** page opens, where you can sign into your account to check their privacy settings.

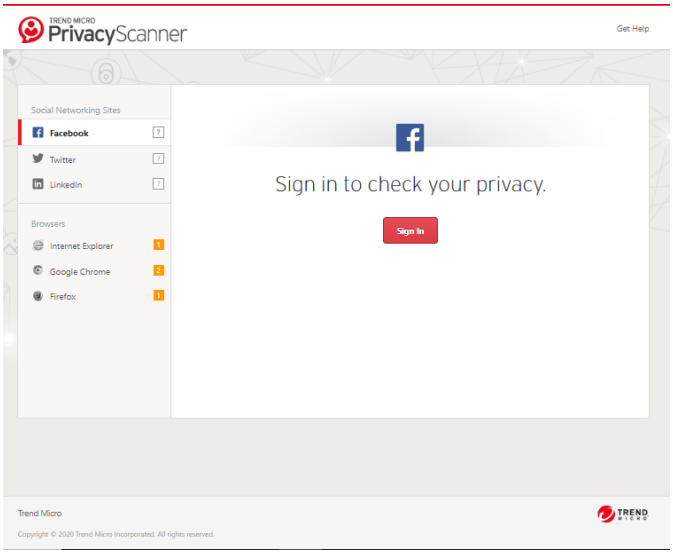


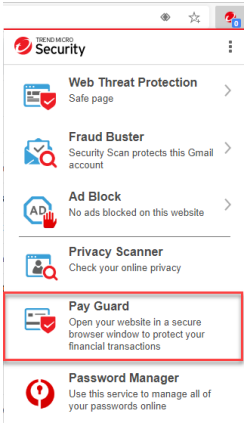

**Figure 81. Privacy Scanner**

3. For more details on using **Privacy Scanner**, go to [Privacy: Privacy Scanner: Social Network Privacy & Web Browser Privacy](#).

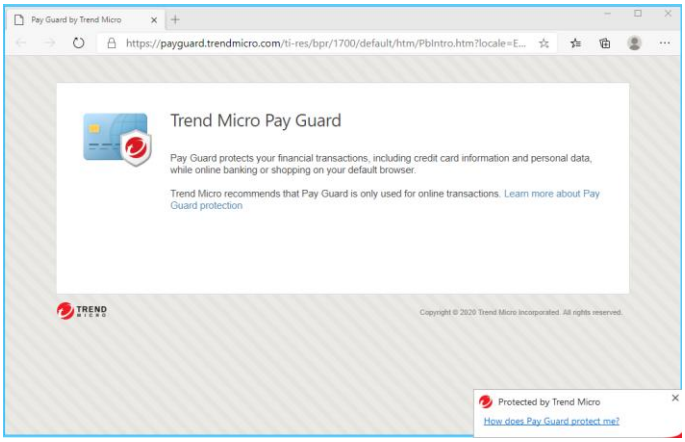
## Pay Guard

**Pay Guard** is a secure version of your default browser. Use Pay Guard for all your financial transactions.

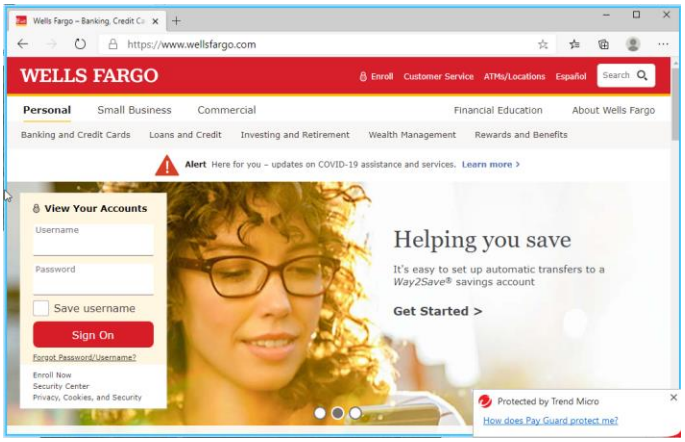
**To use Pay Guard:**




1. Click the **Pay Guard** panel. Pay Guard launches, a hardened version of your default browser.




2. Enter the URL of a financial site; e.g., www.wellsfargo.com.




3. Sign into the financial site, knowing your transactions are secure.
4. Note that you can add **Password Manager** to **Pay Guard**, to assist you in securely signing into your financial accounts.
5. When you install **Trend Micro Maximum Security**, Password Manager is also installed. Then, when you first click **Pay Guard** in the Trend Micro Security for Edge extension, you're prompted to install Password Manager in Pay Guard.

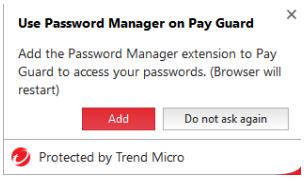



**Figure 82. Use Password Manager on Pay Guard**

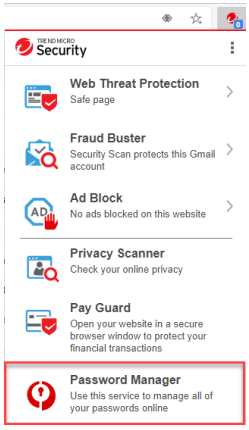
6. Click **Add** to install the Password Manager extension.

## Password Manager

The **Password Manager** item in **Trend Micro Security for Edge** provides direct access to the Password Manager Web **Management Console** after Password Manager is installed, the Trend Micro Security or Password Manager account is activated, and you've created your Master Password.

**Using the Password Manager item to access the Management Console:**

1. To access the Password Manager Web **Management Console,** click the **Password Manager** panel to begin signing in.




2. The **Password Manager Sign In** screen appears.

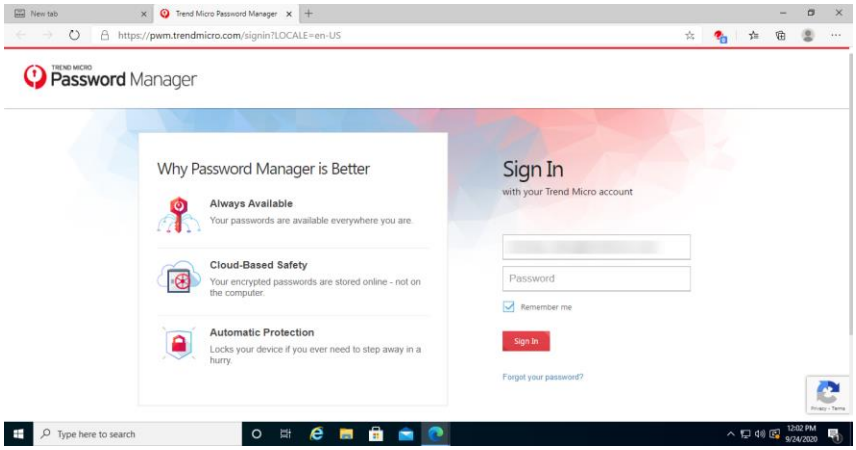



**Figure 83. Sign Into Your Trend Micro Account**

3. Enter the email address and password you used to create your account, and click **Sign In.** The **Management Console** login screen appears.

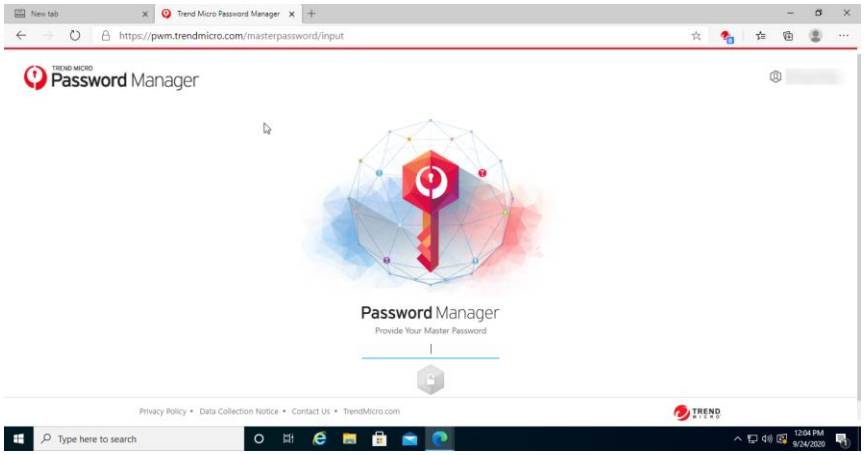



**Figure 84. Management Console Log In**

4. Enter your **Master Password**. The **Management Console** opens.

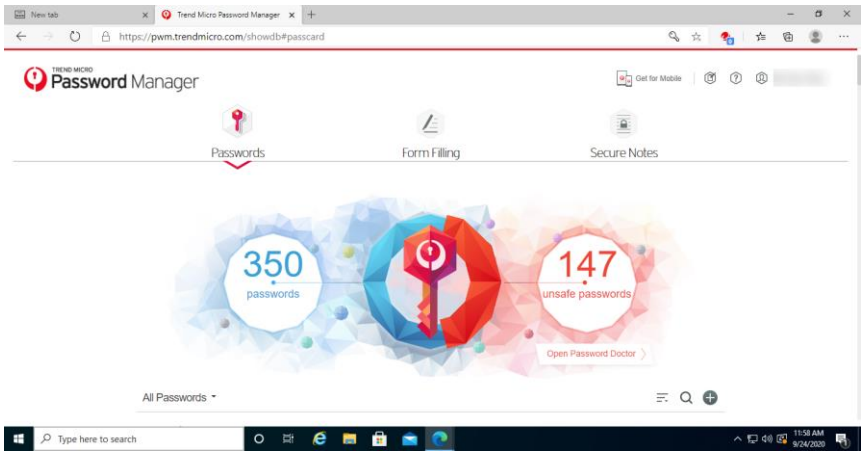



**Figure 85. The Password Management Console with Passwords**

5. You can now manage and edit your passwords.

6. As noted above, to capture and replay passwords, **Trend Micro Password Manager** and its browser extension must also be installed on your computer.

## Enable/Disable Trend Micro Security for Edge

**To Enable/Disable Trend Micro Security for Edge:**

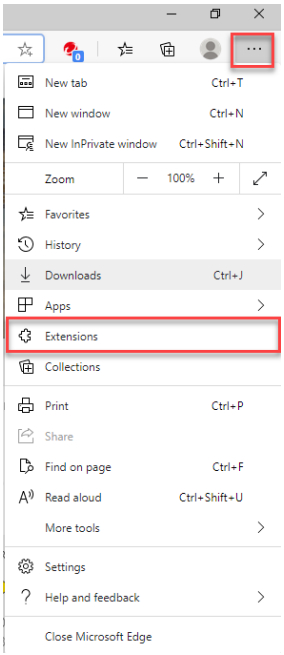



**Figure 86. Edge Tools Icon/Menu**

1. To turn **Trend Micro Security for Edge** on or off, click the **Tools** icon in Edge, then select **Extensions** in the drop-down menu. The **Extensions** page appears.

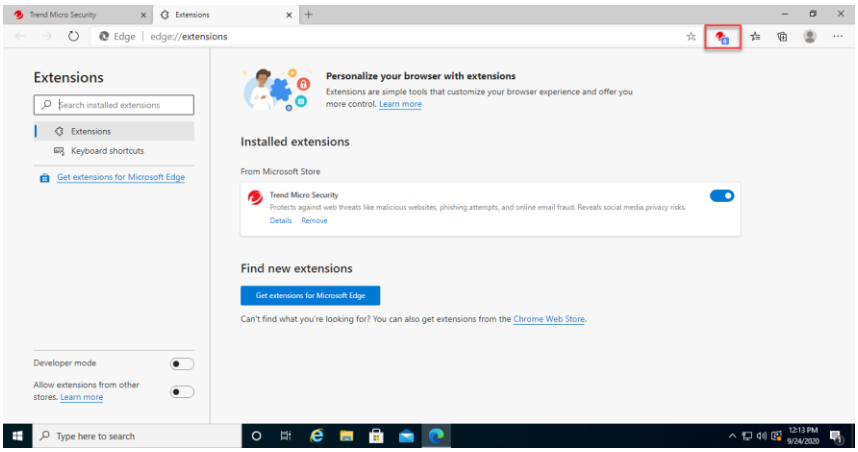



**Figure 87. Edge Tools Menu > Extensions**

2. Slide the toggle to **Off** to turn off **Trend Micro Security for Microsoft Edge**, or to **On** to turn it on. When you toggle it **Off**, the icon (highlighted) disappears from the main menu in Edge.

# Install Trend Micro Toolbar for Google Chrome, Mozilla Firefox, or Internet Explorer

Though Microsoft Edge is now the default browser in Windows 10, you can change the default to Google Chrome or Mozilla Firefox (you have to install them first); or to Internet Explorer (preinstalled with Windows 10). Once you've installed Trend Micro Security, you should then install the **Trend Micro Toolbar** extension in your alternate browser of choice. It lets you **Rate Links** on web pages and at mouseover when searching; protect against fraudulent Gmail and Outlook webmails via **Fraud Buster**; check your **Online Privacy** in Facebook, Twitter, and LinkedIn; and launches **Pay Guard**, a hardened version of your default browser to protect your financial transactions.

The example below uses Google Chrome, but a similar install and activation process occurs for Mozilla Firefox or Microsoft Internet Explorer. (Take note that Microsoft no longer recommends using Internet Explorer, nor the legacy Microsoft Edge, prompting you upon launch to replace them with the new Chromium-based Microsoft Edge.)

**Note:** **Our eSupport page is always available to assist you when installing Trend Micro Toolbar. See How to get Trend Micro Toolbar on your browsers (Trend Micro Security for Windows).**

**To change your default browser:**

1. Once you've installed your alternate browser, you should first select it as the default before you begin using it. To set it as the default, click the **Windows 10 Menu** icon to open it. The menu appears.

**Figure 88. Windows 10 Menu**

2. Click **Settings** icon in the menu. The **Windows Settings** screen appears.

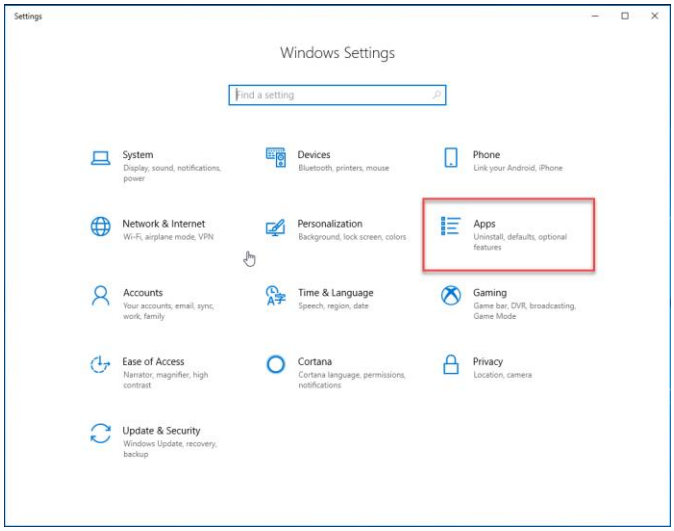



**Figure 89. Settings**

3. Click **Apps**, then **Default apps**, then scroll down to locate **Web Browser**.

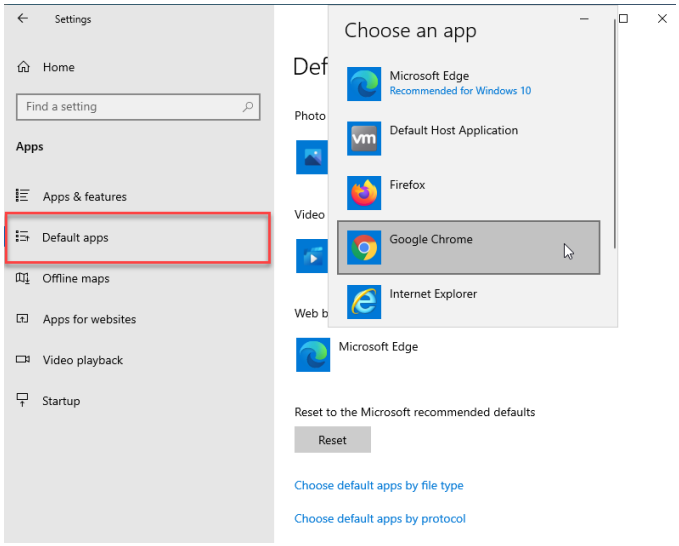



**Figure 90. Settings > System > Default Apps > Web browser**

4. Click **Microsoft Edge**, then scroll down in the popup to your preferred browser; in this example, we select **Google Chrome.**

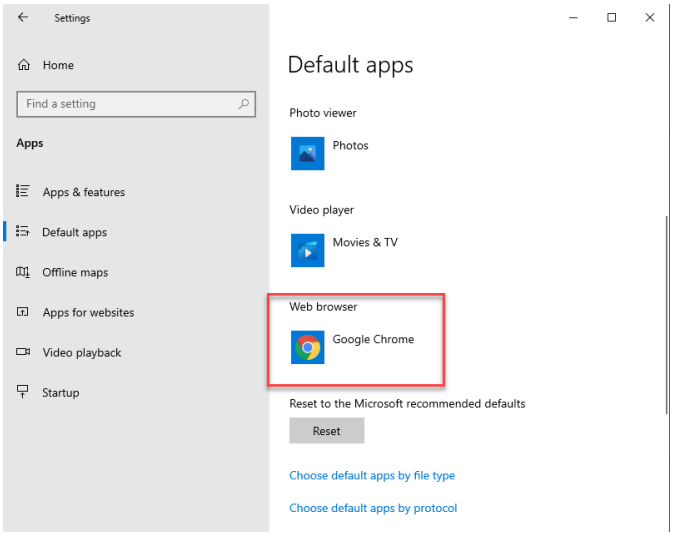



**Figure 91. Google Chrome Now the Default Web Browser**

5. Click **Close (X)** to close the **Settings > Default apps** window.

### To enable Trend Micro Toolbar in Chrome

1. Launch your browser of choice; e.g., double-click **Google Chrome**. Google Chrome loads, and after a short time a popup appears, asking if you wish to **Protect Chrome with the Powerful Trend Micro Toolbar.**

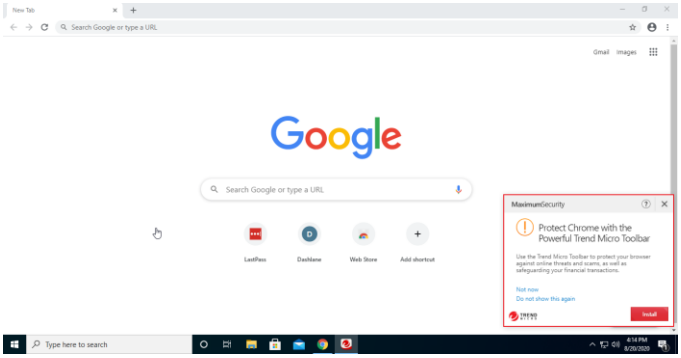



**Figure 92. Protect Chrome with the Powerful Trend Micro Toolbar**

2. Click **Install** in the popup. The **Chrome Web Store** appears, and you're taken to the page to install **Trend Micro Toolbar.**

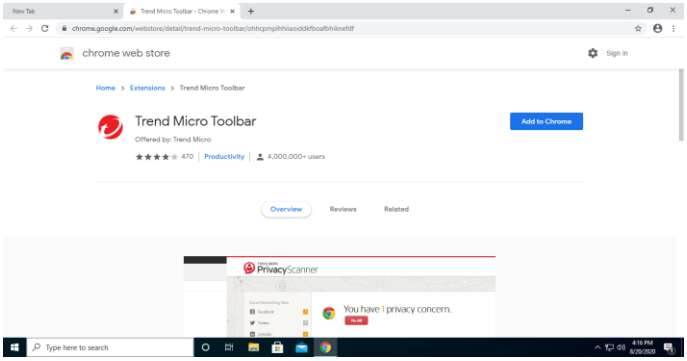



**Figure 93. Add to Chrome**

3. Click **Add to Chrome.** A popup appears, letting you add the extension.

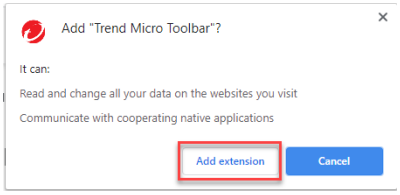



**Figure 94. Add Trend Micro Toolbar**

4. Click **Add Extension** to add it.

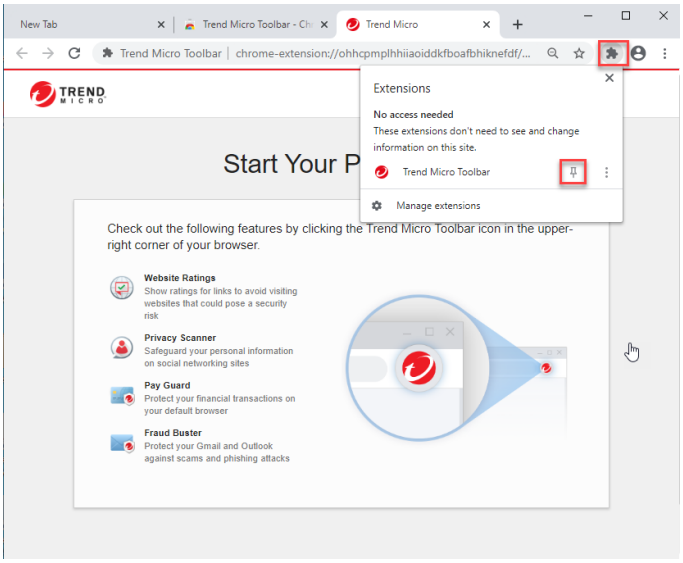



**Figure 95. Start Your Protection**

5. Once it's added, **Start Your Protection** by clicking the **Chrome** extension icon, then the **Trend Micro Toolbar** pin to pin it to Chrome. The **Trend Micro Toolbar** is added to the menu bar, where you can select it to use it.

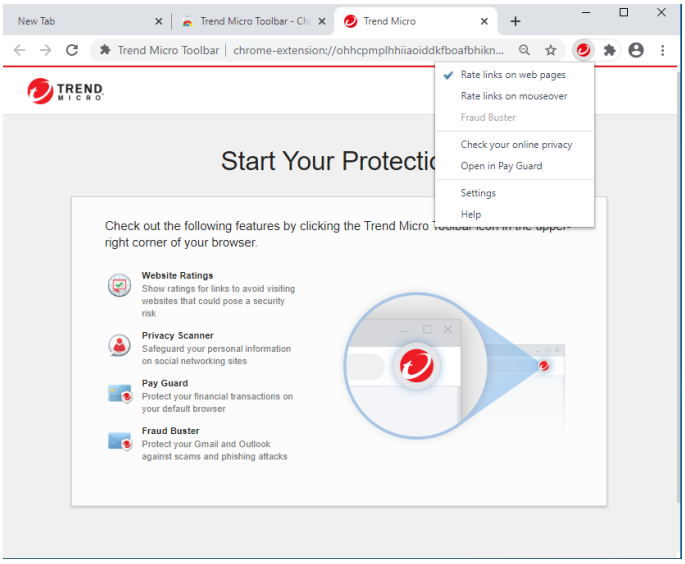



**Figure 96. Trend Micro Toolbar in Chrome**

6. **Trend Micro Toolbar** provides the following features:

   - **Rate links on web pages.** This protects you when you're browsing, rating links for web threats and blocking you when a webpage is dangerous.
   - **Rate links on mouseover.** This protects you in search results, allowing you to mouse over a result to see if it's safe.
   - **Fraud Buster.** This protects you in Gmail and Outlook Webmail for fraud perpetrated through phishing emails.
   - **Check your online privacy.** This lets you check your privacy settings in Google, Twitter, and LinkedIn, or in your Internet Security, Google Chrome, or Mozilla Firefox browser. This item it active in **Trend Micro Internet** and **Maximum Security**.
   - **Open in Pay Guard.** This launches a hardened version of your browser, for use when banking or buying.
   - **Settings.** This provides access to the Trend Micro Toolbar Settings, to choose the level of protection you want.
   - **Help.** This provides help when using Trend Micro Toolbar.

7. See the relevant sections in this guide for more details on using the specific feature.

**To enable Trend Micro Toolbar in Pay Guard:**

1. You can also install **Trend Micro Toolbar** in **Trend Micro Pay Guard**, which is a hardened version of your default browser, tailored to keep you safer when banking or shopping online. (Our example here again shows Chrome. The same process should be followed for Firefox.)

2. Double-click the **Pay Guard** icon on your desktop to launch it.

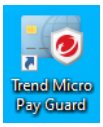



**Figure 97. Trend Micro Pay Guard Desktop Icon**

3. When **Pay Guard** launches, copy this hyperlink into the Pay Guard URL field: **Trend Micro Toolbar** to return to the **Chrome Web Store** page and repeat the process above to install **Trend Micro Toolbar** into **Trend Micro Pay Guard**, activate it, then pin it to the Menu bar.

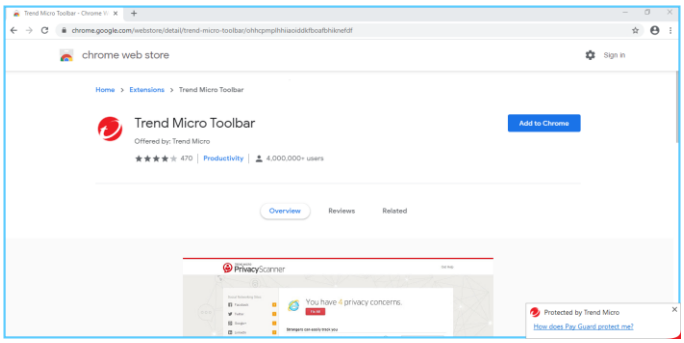



**Figure 98. Trend Micro Pay Guard > Trend Micro Toolbar**

## Rate Links on Web Pages

**Using Rate Links on Web Pages:**

1. Ensure **Rate links on web pages** is checked in **Trend Micro Toolbar.**

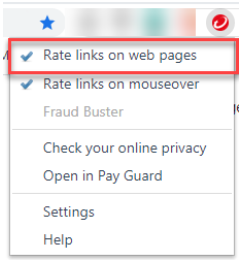



**Figure 99. Rate Links on Web Pages**

2. If you inadvertently navigate to a dangerous web page, you'll be blocked by the web threat protection in **Trend Micro Toolbar.**

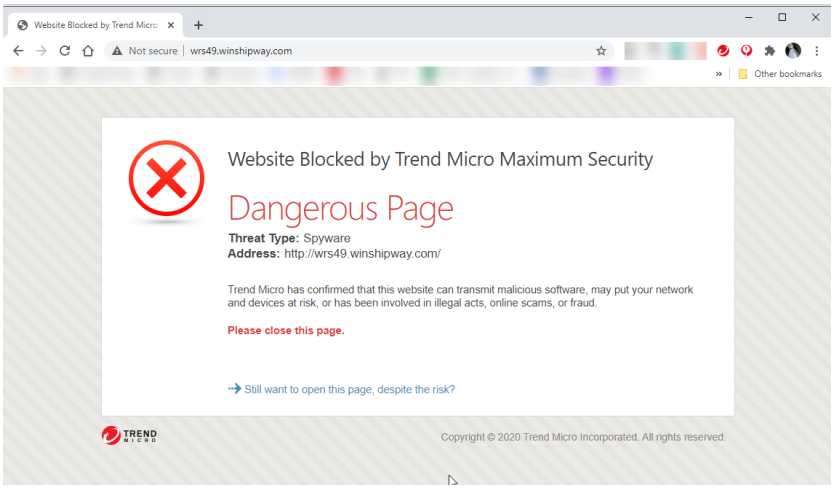



**Figure 100. Website Blocked**

## Rate Links on Mouseover

**Using Rate Links on Mouseover:**

1. Ensure **Rate links on mouseover** is checked.

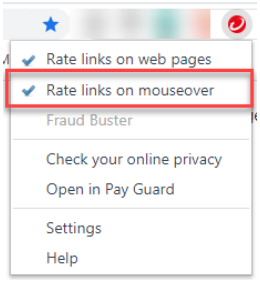



**Figure 101. Rate Links on Mouseover**

2. Now, if you conduct a search and the search results reveals malicious sites, **Rate Links on mouseover** will rate the danger of the website in the search results, as **Safe, Untested,** or **Dangerous**. If you click the link to the Dangerous website, you'll be blocked.

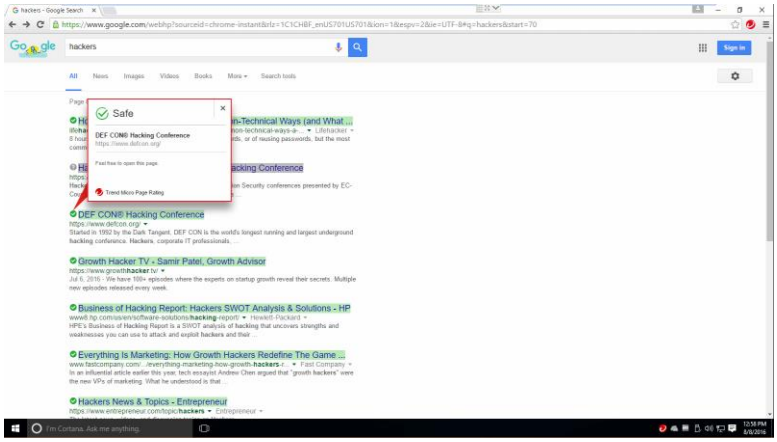



**Figure 102. Google Chrome > Search Results Showing Safe Pages**

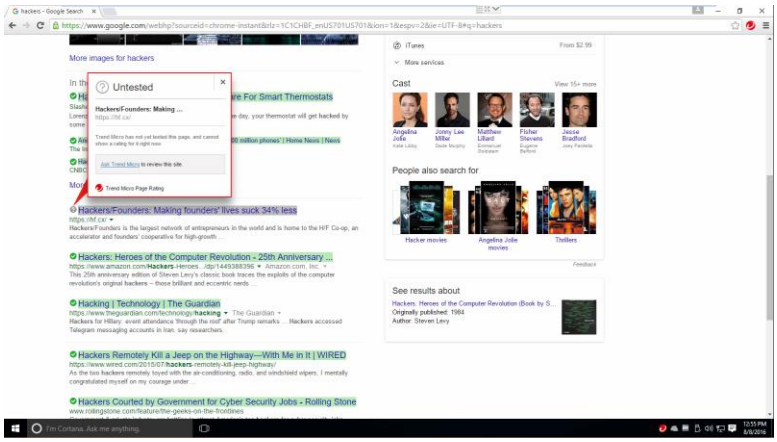



**Figure 103. Google Chrome > Search Results Showing Untested Page**

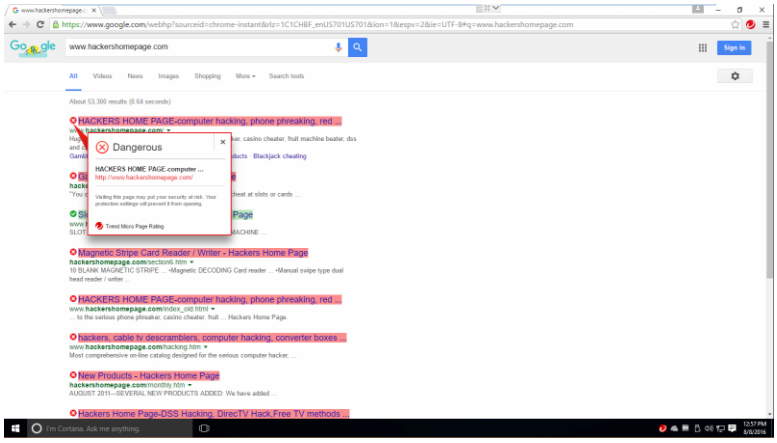



**Figure 104. Google Chrome > Search Results Showing Dangerous Pages**

## Fraud Buster for Gmail and Outlook Webmail

More and more scam emails these days may contain no obvious malicious URLs or attachments but can nonetheless be a threat, using social engineering to snare the unsuspecting user. However, such emails can't be detected by traditional email security technology.

**Fraud Buster** is designed to deal with this type of scam email, using artificial intelligence (AI) technology to identify the topic and to understand the intention of the scam. As part of **Trend Micro Toolbar**, **Fraud Buster** protects Gmail and Outlook webmail in Chrome, Firefox, and Internet Explorer. The example below uses Gmail in Chrome to show the setup.

**To enable Fraud Buster:**

1. **Fraud Buster** requires first that you log into your Gmail or Outlook webmail account.

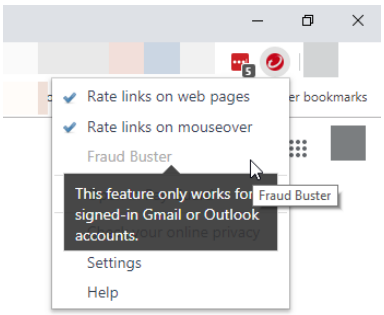



**Figure 105. Sign in to Gmail or Outlook to Enable Fraud Buster**

2. For example, sign into your Gmail account in Chrome.

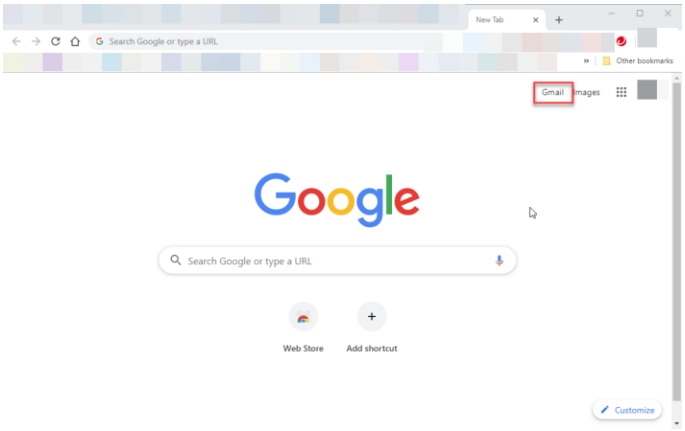



**Figure 106. Gmail Button in Chrome**

3. Then, on the Google home page, click **Gmail** to open your **Gmail** webmail. A popup appears for you to **Protect Your Webmail.**

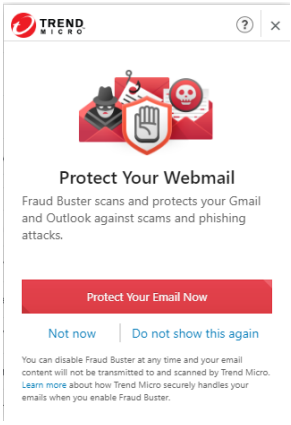



**Figure 107. Protect Your Webmail**

4. Click **Protect Your Email Now.** Another popup appears, describing how **Fraud Buster** protects your Gmail and Outlook.com against scams and phishing attacks by sending your email content to Trend Micro to scan.

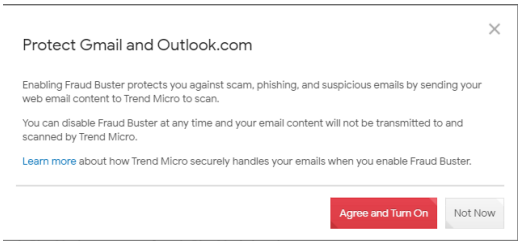



**Figure 108. Protect Gmail and Outlook.com**

5. If you agree to it, click **Agree and Turn On.**

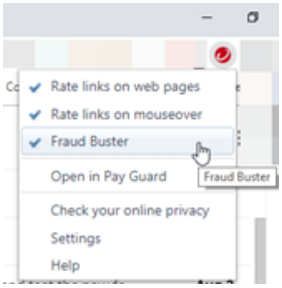



**Figure 109. Gmail Protected by Fraud Buster | Active in Trend Micro Toolbar**

6. **Fraud Buster** is now enabled and you can see it active in the **Trend Micro Toolbar**.
7. Your Gmail (or Outlook.com) webmail will now be scanned for potential scams and you'll be alerted with a warning popup when you open a scam email, telling you to not follow any instructions contained in the email.

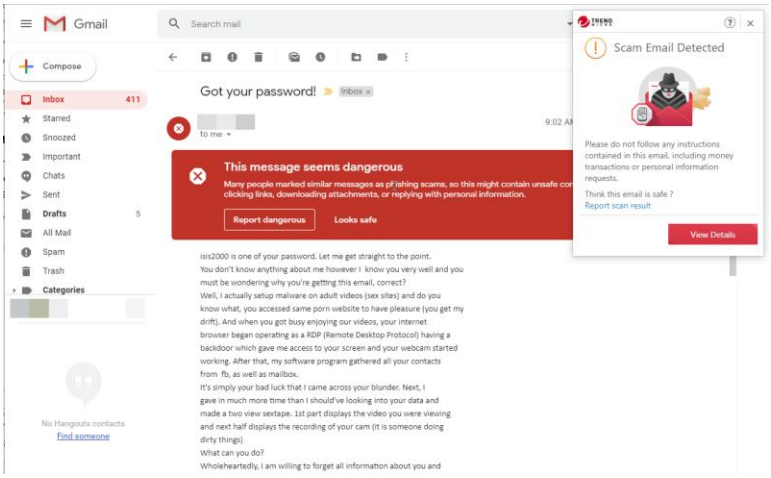



**Figure 110. Scam Email Detected**

8. You can click **Report Dangerous** to report the scam webmail or **Looks Safe** to bypass the warning (not recommended). In this example, click **View Details** in the popup warning to get more details about the scam.

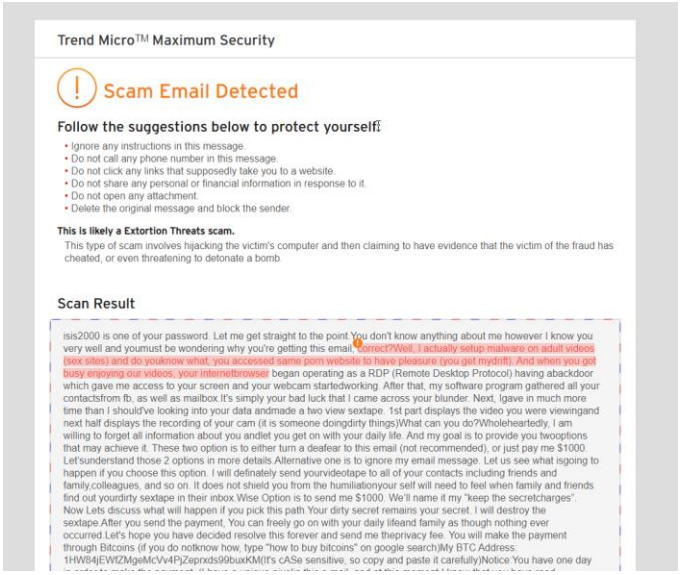



**Figure 111. Scam Email Detected: Details**

9. Follow Trend Micro's instructions to better protect yourself from scams; or contact Trend Micro to get more support. When done, close the **Details** window and scam email, then delete the scam email from your inbox.

## Check Your Online Privacy

Your privacy is important on Social Media, but you may be sharing too much information to keep yourself safe. When using **Trend Micro Internet Security** or **Maximum Security**, **Trend Micro Toolbar** lets you **Check your online privacy** on Facebook, Twitter, or LinkedIn, or in the main alternate Windows browsers: **Internet Explorer, Google Chrome,** or **Mozilla Firefox.**

**To Check your online privacy:**

1. Click **Check your online privacy** in **Trend Micro Toolbar.**

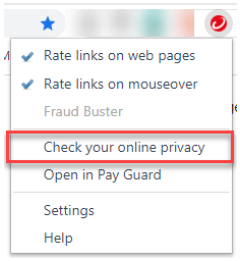



**Figure 112. Check Your Online Privacy**

2. A window opens in your browser and lets you sign into your Social Networking account, or to test your privacy settings in your browser(s).

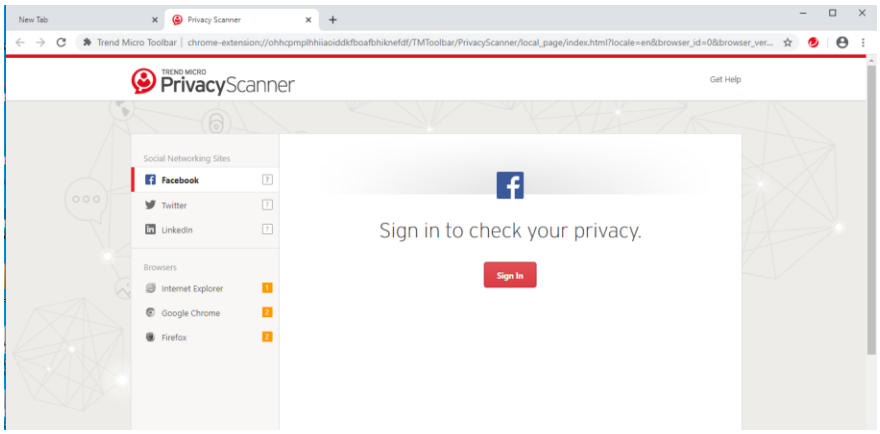



**Figure 113. Sign In To Check Your Privacy**

3. For more details, see the section **Privacy: Privacy Scanner: Social Network Privacy & Web Browser Privacy.**

## Open in Pay Guard

**Pay Guard** is a hardened version of your default browser to increase your security when banking or shopping online.

**To open a website in Pay Guard:**

1. Navigate to a banking or shopping website, then click **Open in Pay Guard** in the **Trend Micro Toolbar.**

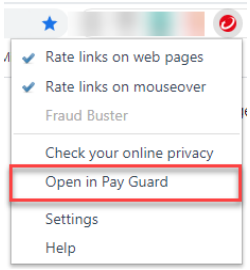



**Figure 114. Open in Pay Guard**

2. **Pay Guard** loads the site in a protected version of your browser.

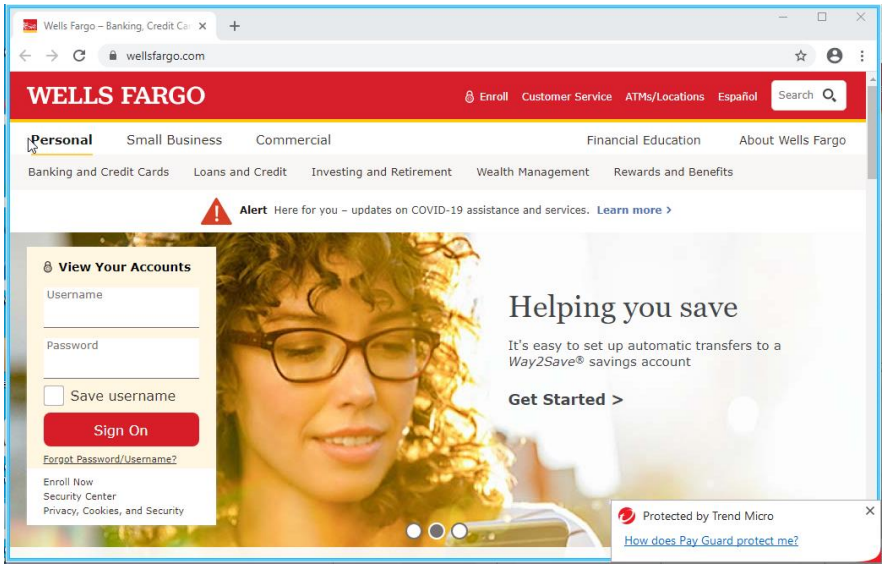



**Figure 115. Financial Site in Pay Guard**

3. Sign into the website, knowing your transactions are secure. For more details go to the section **Privacy: Pay Guard**.

## Settings

You can set the **Protection Strength** of Trend Micro Toolbar in the **Settings** screen of the **Trend Micro Security Console.**

**To configure Protection Strength in Trend Micro Toolbar:**

1. Click **Settings** in the **Trend Micro Toolbar.**

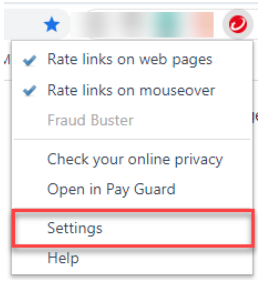



**Figure 116. Settings**

2. The **Trend Micro Security Console** loads and presents the **Settings** page.

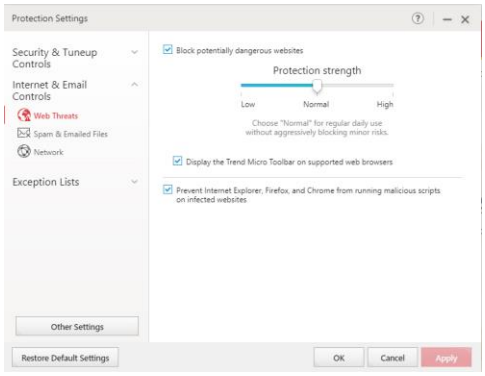



**Figure 117. Protection Strength**

3. Set your **Protection Strength** to **Low, Normal, or High.**
4. Check/Uncheck **Display the Trend Micro Toolbar on supported web browsers.**
5. Check/Uncheck **Protect Internet Explorer, Firefox, and Chrome from running malicious scripts on infected websites.**
6. Click **Apply** to apply your changes.

## Help

You can get Help using Trend Micro Toolbar, for installation and instruction purposes.

**To get Help with Trend Micro Toolbar:**

1. Click **Help** in the **Trend Micro Toolbar.**

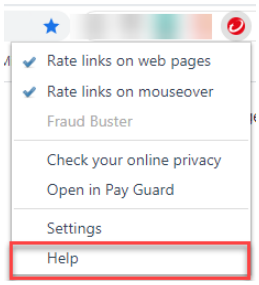



**Figure 118. Help**

2. A **Help** window appears in your browser, where you can learn more about how **Trend Micro Toolbar** works.

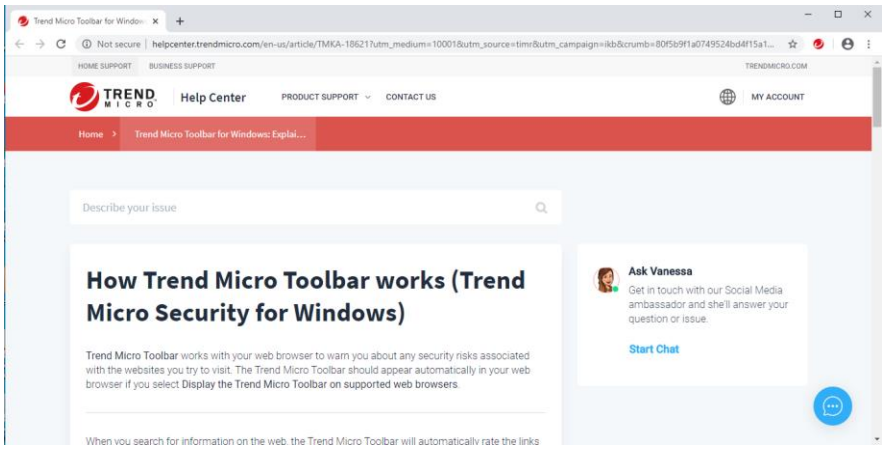



**Figure 119. How Trend Micro Toolbar Works**

3. Scroll down the Help page to get information about **Searching, Website Ratings,** and other **Trend Micro Toolbar Options**.

## Enable/Disable Trend Micro Toolbar

You can enable/disable Trend Micro Toolbar, though Trend Micro recommends that you keep it enabled to increase your security.

**To enable/disable Trend Micro Toolbar:**

1. In this Chrome example, select the **Tools** icon, then navigate to **More tools > Extensions** in the dropdown menus.

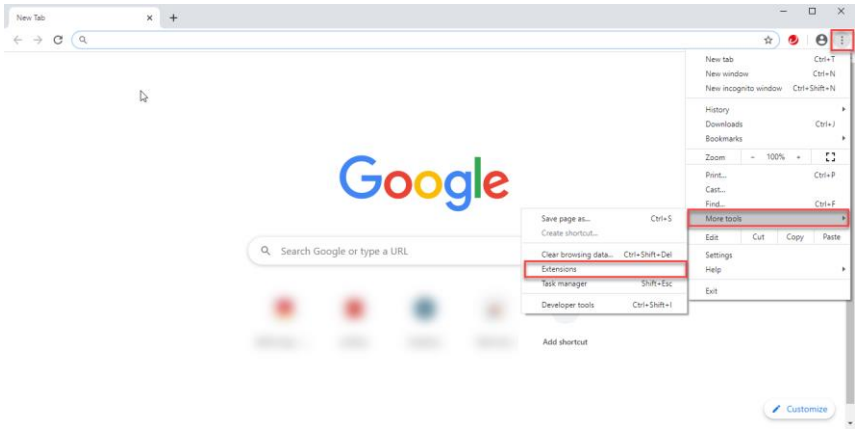



**Figure 120. Accessing Extensions in Chrome**

2. When the **Extensions** page displays, locate the **Trend Micro Toolbar** extension to toggle the toolbar **On/Off**, get more **Details**, or **Remove** the extension.

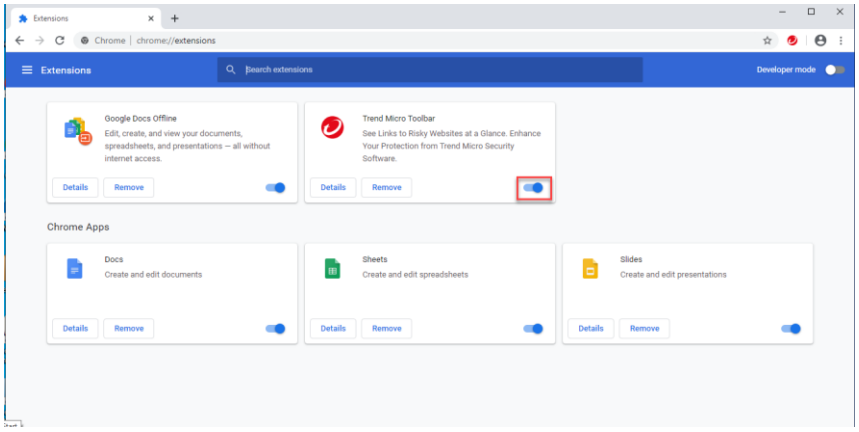



**Figure 121. Toggle Trend Micro Toolbar On/Off**

# Set Up Parental Controls

See the **Family: Parental Controls** section to learn how to set up **Parental Controls** in **Trend Micro Internet Security** and **Maximum Security.**

# Chapter 3: Trend Micro Security Overview

In the following chapters, we'll walk through each edition of Trend Micro Security, explaining the key features provided in each. In this chapter, we'll give you a quick overview of some easy-to-use functions.

**Note:** **Since each more advanced edition of Trend Micro Security includes the features of the prior edition, but adds additional ones, you should read all chapters in this guide from *front to back* to fully understand how to use the complete set of features in Trend Micro Internet and Maximum Security.**

## Quick Start: The Trend Micro Security Console

All editions of Trend Micro Security provide essentially the same **Console**, with additional features as you step up from **Trend Micro Antivirus+** to **Internet Security** and **Maximum Security.**

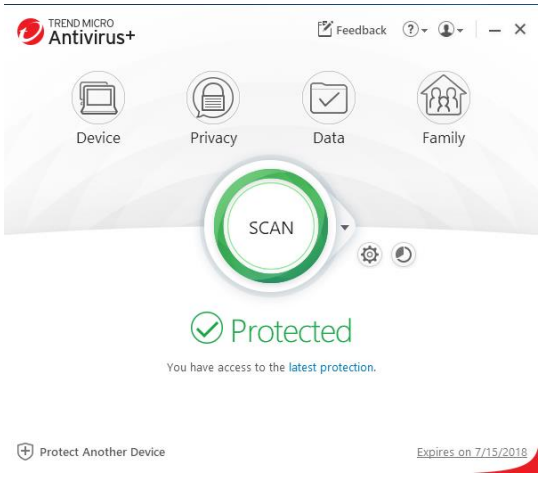



**Figure 122. Trend Micro Antivirus+ Security Console**

All editions of Trend Micro Security allow you to scan on-demand using **Quick, Full,** or **Custom** scans, and each lets you view security reports. We'll quickly review these features in the following sections.

## Quick Start: Conducting On-Demand Scans

By default, Trend Micro Security activates a **real-time scan** when it is installed. This is always present in memory, to proactively protect you from real-time threats. Threats are caught as they try to enter memory or touch the hard drive, preventing infections. This includes protection against ransomware, which may infect you from dangerous websites or emails.

Trend Micro Security also provides a **disk scan**—which you can execute on-demand or by schedule—that utilizes Trend Micro Smart Scan technology on the client when it scans your

hard drive. This references Trend Micro's file reputation services in the cloud—part of the Smart Protection Network—for a shorter "time-to-protect."

Unlike other local-protection-based products that require you to frequently update a large local signature database on your computer, Trend Micro Security updates the signature database mainly on Trend Micro Servers in the cloud, so all consumers of the Smart Protection Network are instantly protected whenever the online database is updated. Other cloud-based and local Trend Micro technologies correlate threat data of different kinds, since modern threats can simultaneously use multiple techniques to infect your computer.

Smart Scan reduces network bandwidth usage (for updating/downloading signatures), while saving disk space and memory.

## Scan Your Computer's Disk

Scanning is a simple process to execute, though users are recommended to initiate a manual scan when they are not doing other tasks.

**To scan your computer disk:**

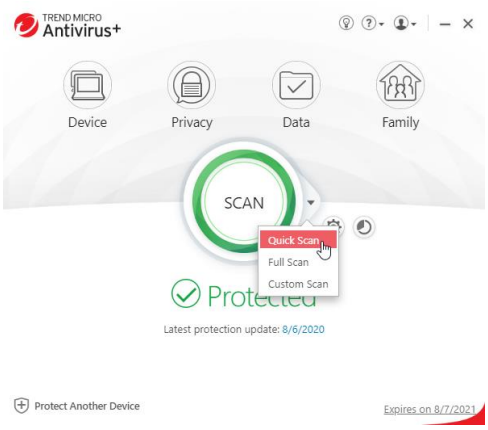



**Figure 123. Quick | Full | Custom Scan Menu**

Trend Micro Security provides a **Scan** Tool on the console (shown above) which can be used in two ways:

1. Click the center of the circular **Scan** tool to execute a **Quick Scan**.
2. Use the **Scan Options** popup menu on the right side of the **Scan** tool to select among the various options:
   - A **Quick Scan** conducts a scan of those directories on your system that are most likely to be infected.
   - A **Full Scan** conducts a full scan of your system.
   - A **Custom Scan** lets you designate which parts of your system you wish to scan.

## Quick Scan and Full Scan

**To conduct a Quick Scan or a Full Scan:**

1. To conduct a **Quick Scan**, click the **Scan** button on the main console, or optionally select **Quick Scan** or **Full Scan** from the **Scan Options** popup menu. A window appears, showing the **Quick** or **Full Scan in Progress** and the percentage completed. Scans can kick off messages when malware is quarantined or deleted.

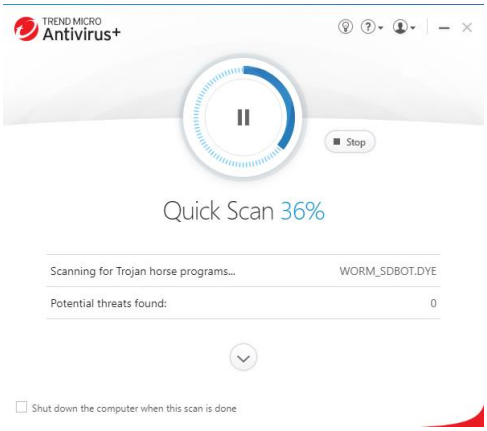



**Figure 124. Quick Scan in Progress**

2. You may stop the scan by clicking the **Stop** button. You may also select **Shut down the computer when this scan is done.**

3. When the scan has completed, a **Scan Results** screen appears, showing **File Scanned**, as well as **Threats resolved.**

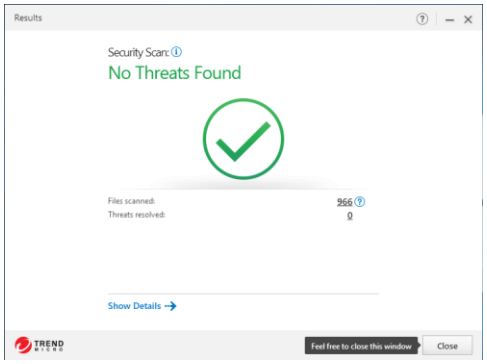



**Figure 125. Scan Results**

4. Click **?** near the number of **Files scanned** to obtain more details on the files scanned.

5. Click **Show Details** for more details on the threats found and actions taken. The **Details** screen appears.

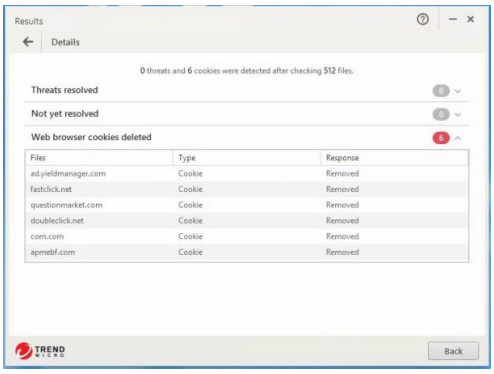



**Figure 126. Details**

6. Click each of the collapsible panels in turn to show the **Details** tables, which include file names, types, and responses to the threats.
7. Click **Back** to close the **Details** window, then **Close** to close the **Scan Results** window.

## Custom Scan

**To conduct a Custom Scan:**

1. Choose **Custom Scan** from the **Scan Options** popup menu. A dialog appears, letting you **Select Targets** you wish to scan.

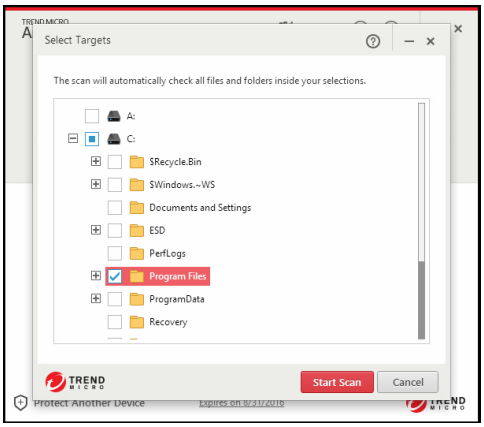



**Figure 127. Select Targets**

2. Expand any tree by clicking the **+ (Plus)** signs, then check the checkbox for the chosen target(s).
3. Click **Start Scan** to start the scan.
4. When the scan has completed, the **Scan Results** and **Details** screens appear in the same format as **Quick** and **Full Scans.**

## Intensive Scan

Trend Micro Security automatically performs an **Intensive Scan** whenever a **Quick, Full, Custom, Scheduled Scan,** or **"Smart Schedule"** scan detects a high amount of malware on your computer.

**Note:** **In the *real world,* Trend Micro Security does not allow a large virus data set to get onto your computer. To obtain this condition artificially, you have to dump a large collection of malware files onto an unprotected system *before you install Trend Micro Security;* or you would have to turn off all the proactive features, such as the real-time scan, which would prevent such a large infection from occurring in the first place.**

**To activate an Intensive Scan on a previously badly infected computer:**

1. Click the **Scan > Quick Scan** tool to begin a **Quick Scan**. The **Quick Scan** process begins.

**Figure 128. Quick Scan in Progress (TM Maximum Security)**

2. When the scan detects a large volume of malware, the **Quick Scan** stops and an **Intensive Scan** starts.

**Figure 129. Intensive Scan in Progress**

3. Note that the scan wheel color changes to **red** to indicate that an **Intensive Scan** is in progress. You can get more information about what triggered the scan by clicking **What triggered the Intensive Scan?**

# Quick Start: Viewing Security Reports

Trend Micro Security allows you to view **Security Reports** at the click of a button. The reports provide a wealth of detail on the dates and types of threats blocked. You can also generate a **Root Cause Analysis Report** to investigate the source of an infection and the effects upon your system.

**Note:** **All versions of Trend Micro Security produce a security report that tells you how many and what kinds of viruses, spyware, and web threats it detected during real-time and on-demand scans. Higher editions than Antivirus+ provide more information in their Security Reports.**

**To View a Security Report:**

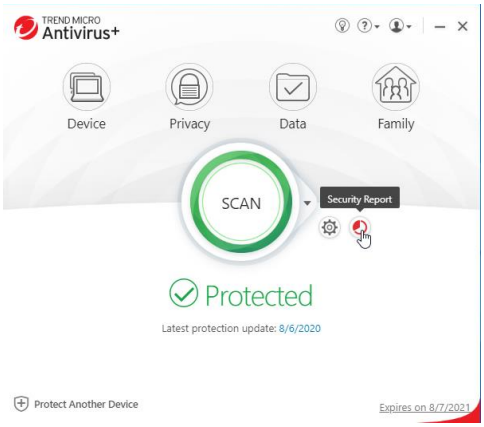



**Figure 130. Security Report**

1. Click the **Security Report** button on the **Trend Micro Security Console**. The **Security Report** screen appears. (Note that if you've created a password to secure your settings, you'll be asked to enter this password before the **Security Report** is displayed.)

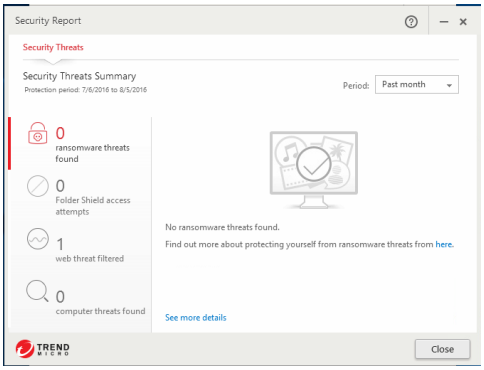



**Figure 131. Security Report (Antivirus+ Security)**

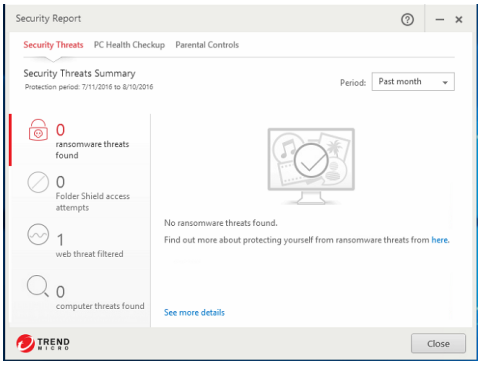



**Figure 132. Security Report (Internet Security)**

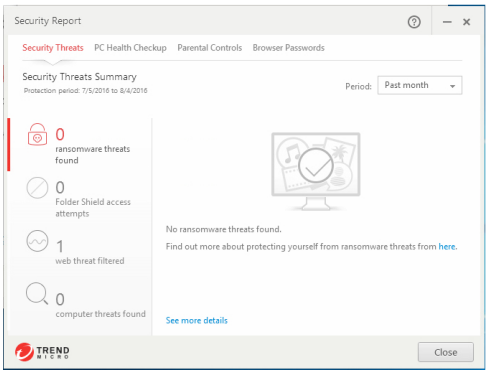



**Figure 133. Security Report (Maximum Security)**

2. The **Security Report** provides the following data:
   - **Security Threats** – The number of web threats, viruses, spyware, ransomware, and suspicious software found. (All editions)
   - **PC Health Checkup** – Shows the space and startup time saved and the privacy data safety confirmed, and includes a check for potentially incompatible programs. (Internet Security and higher)
   - **Parental Controls** – Shows a summary of the top websites blocked. (Internet Security and higher)
   - **Browser Passwords** – The number of passwords saved in browsers (a privacy risk). (Maximum Security)
3. Use the **Period** popup menu in the upper right-hand corner to designate the period the report will cover.
4. Select **See more details about your protection** from any of the four main screens to obtain logs pertaining to that type of protection.

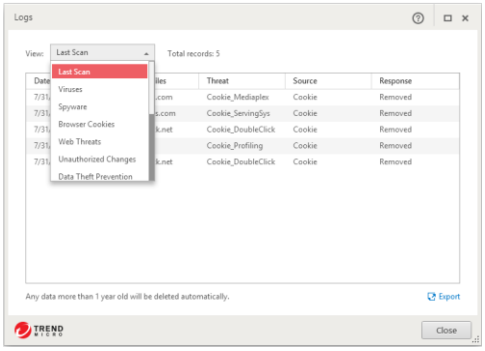



**Figure 134. Logs**

5. Double-click an item in the table to view details on the specific threat.

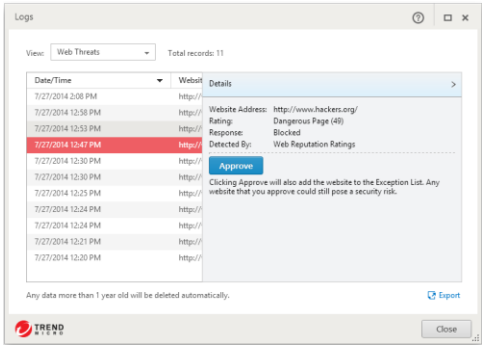



**Figure 135. Logs > Item Details**

6. Click **Approve** to add items to the **Exception List.**
7. Click **Export** in the lower right-hand corner to export the logs in .CSV or .TXT format.
8. When an item in a log warrants a deeper look, Trend Micro Security will provide a link to show more details on the source of the infection.

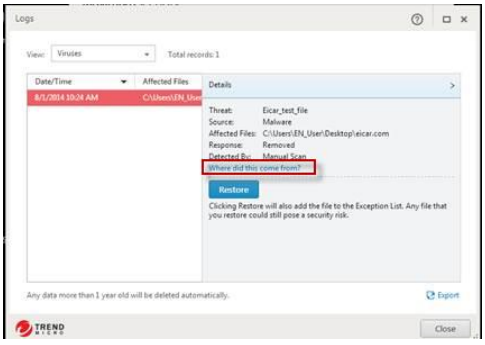



**Figure 136. Where did this come from?**

9. Click **Where did this come from?** to generate a **Root Cause Analysis Report.** When the report generates, it displays in graphic format.

**Figure 137. Root Cause Analysis Report**

10. The **Root Cause Analysis Report** maps the root cause and triggering event(s) graphically, using **Process, Website, File, Library,** and **Group** icons to show you items involved in the infection chain. Use the **Root Cause Analysis Report** to analyze the source of infections, so you can help prevent them in the future.

# Chapter 4: Trend Micro Antivirus+ Security

This chapter provides detailed instructions for configuring and using Trend Micro Antivirus+ Security. All the features presented here are also included in Trend Micro Internet Security and Trend Micro Maximum Security.

## Protection Overview

**Trend Micro™ Antivirus+ Security** provides essential protection for customers against viruses, spyware, web threats, and other malware threats, including bad links on social networking sites and ransomware.

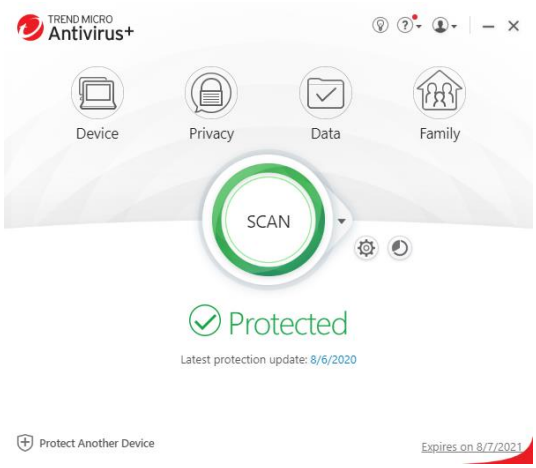



**Figure 138. Trend Micro Antivirus+ Security Console**

**Note:** **Trend Micro Antivirus+ Security Console Main Features:**

**Device: Security Settings | Mute Mode | Protect Another Device**

**Privacy: Social Networking Protection | Pay Guard**

**Data: Folder Shield**

**Family: Keep Your Family Safe Online - Upgrade Now**

**KEY MALWARE PROTECTIONS FOR TREND MICRO ANTIVIRUS+ SECURITY**

**Antivirus and Antispyware**

**Trend Micro Antivirus+ Security** provides essential protection against viruses; that is, any malicious program that can replicate itself and infect your computer. Antivirus+ also protects you from a broad range of other malware, including worms, Trojans, bots, and rootkits. It also provides protection from spyware; that is, any program that installs itself in the background and gathers information about you or your computer without your knowledge. Since browser cookies can act like spyware, Antivirus+ will delete cookies as well.

**Windows Firewall Booster and Wi-Fi Protection**

The Windows Firewall Booster provides additional network-level protections, including a Network Virus Scan and Anti-Botnet feature. The Firewall Booster is automatically activated for increased network security. Antivirus+ also provides authentication for Wi-Fi networks, displaying a warning when connected to potentially unsafe wireless networks or hotspots.

**Anti-Spam**

Antivirus+ includes anti-spam in its list of features. Users of POP3 e-mail can be protected from spammers, stopping unsolicited advertisements and other unwanted bulk email. Trend Micro Security's anti-spam function taps into the email reputation services of the Smart Protection Network. Trend Micro Security Antivirus+ also protects you from threats in files attached to email messages. **Fraud Buster** also provides anti-spam and WTP protection for Gmail and Outlook webmail.

**Unauthorized Change Prevention**

Trend Micro Security includes behavior monitoring in its list of security protections. Unauthorized changes to system settings and other suspicious behavior can be blocked, as well as autorun programs on portable drives. Antivirus+ includes the ability to switch your protection level automatically, to aggressively eliminate programs that pose even a small risk of bad behavior. And the increased protection against ransomware that Folder Shield provides helps protect your computer and files from encryption or blocked access and the extortion that comes with ransomware. All editions of Trend Micro Security provide ransomware protection and Folder Shield.

**Web Threat Protection**

The majority of threats nowadays come from the web, when you're simply browsing the Internet or visiting a site. However, attacks may also begin with a phishing email that uses social engineering techniques to coax you to click a URL link in the email. You then may be taken to a website that secretly harbors malicious threats, which either steals your personal data or infects you with malware.

Antivirus+ proactively protects you from a variety of these web threats, so that they never touch your computer. To provide thorough protection from and rapid response times to emerging threats, Antivirus+ uses the Trend Micro Smart Protection Network cloud-client security infrastructure along with a combination of cloud-based web, file, and email reputation services. It also employs real-time scans of what's in memory and on disks. Antivirus+ also blocks malicious links and image spam in emails, including Google and Outlook webmail with Fraud Buster.

**Privacy**

**Social Networking Protection** in Trend Micro Antivirus+ Security is also enabled by the Web Threat Protection function. See risk ratings for Facebook, Twitter, LinkedIn, MySpace, Pinterest, Mixi, and Sina Weibo. Mouse over URLs to get further details on the website. In Facebook, warn your friends of bad URLs on their pages, so they can delete them.

**Pay Guard** protects your financial transactions when you're banking or shopping online using your default browser.

# Device: Security Settings: Security & Tuneup Controls > Scan Preferences

Upon install, Trend Micro Antivirus+ Security chooses a group of default settings to immediately protect the user. However, users can modify settings as they wish. Antivirus+ Security keeps its controls simple and suitable for the everyday user.

**To modify Security & Tuneup Controls settings:**

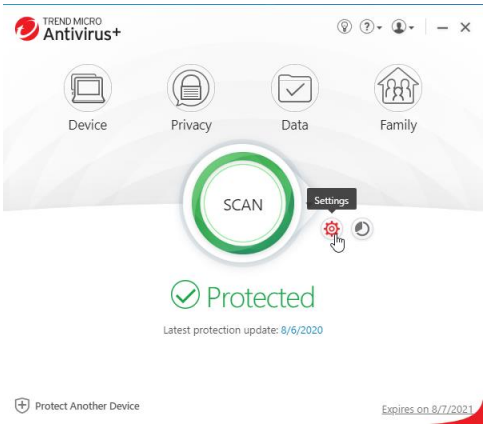



**Figure 139. Console > Settings Tool**

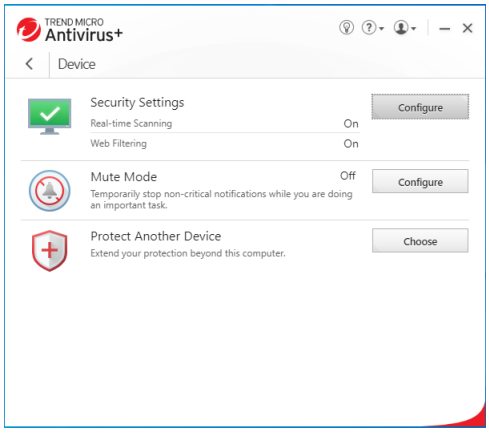



**Figure 140. Device > Configure**

1. Click the **Settings** tool in the **Console**; or click the **Device** button, then **Configure** in the **Security Settings** panel. The **Protection Settings** screen appears, with **Security & Tuneup Controls > Scan Preferences** selected by default in the **Command Menu**.

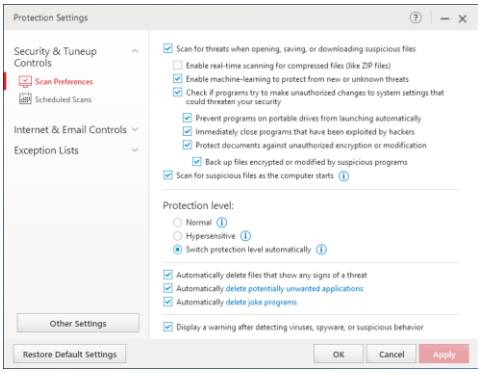



**Figure 141. Scan Preferences**

2. The following **Scan Preferences** are displayed. Check or uncheck to change a setting.

- **Scan for threats when opening, saving, or downloading suspicious files.** This is the real-time scan that protects you at all times when you're using your computer. This is enabled by default.
    - **Enable real-time scanning check compressed files (like ZIP files).** This is disabled by default. Checking the checkbox enables the item, but the deeper scan uses more CPU cycles.
    - **Enable machine-learning to protect from new or unknown threats.** This is enabled by default. New or unknown threats, such as ransomware, will be removed upon detection; or when suspicious software tries to execute, it will be blocked.

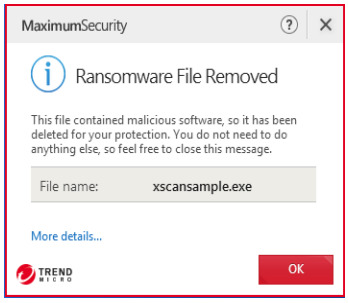



**Figure 142. Ransomware File Removed**

[Maximum Security example]

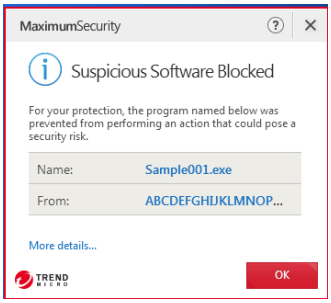



**Figure 143. Suspicious Software Blocked from Executing**

[Maximum Security example]

    - **Check if programs try to make unauthorized changes to system settings that could threaten your security.** This is enabled by default.
        - **Prevent programs on portable drives from launching automatically.** This is enabled by default.
        - **Immediately close programs that have been exploited by hackers.** This is enabled by default.

        - **Protect documents against unauthorized encryption or modification.** This protects against ransomware and is enabled by default.

- **Scan for suspicious files as the computer starts.** Key security components begin working even before Microsoft Windows has finished loading—before threats have a chance to attack.
- **Protection Level**. This behavior monitoring function is enabled by default to switch from Normal to Hypersensitive only when needed, but you can change this setting.
    - **Normal -** Detects and stops security threats based on clearly risky behavior.
    - **Hypersensitive -** Aggressively eliminates programs even if they only pose a small risk of bad behavior.
    - **Switch protection level automatically** - Increases the protection level only when you need it. This is the default setting.
- **Automatically delete files that show any signs of a threat**. This is enabled by default, to automatically delete threatening files.
- **Automatically delete potentially unwanted applications.** This is enabled by default.
- **Automatically delete joke programs.** This is enabled by default.
- **Display a warning after detecting viruses, spyware, or suspicious behavior.** This is enabled by default. Trend Micro Security is selective when using pop-ups; it's never overly intrusive.

3. If you wish, click **Restore Default Settings** at any time (in this and any subsequent screens) to restore default settings to their factory condition.
4. Click **Apply** to apply your changes, then **OK** to close the **Protection Settings** window.

# Device: Security Settings: Security & Tuneup Controls > Scheduled Scans

**To modify Scheduled Scan preferences:**

1. Click **Security & Tuneup Controls > Scheduled Scans**. The schedule options panel displays.

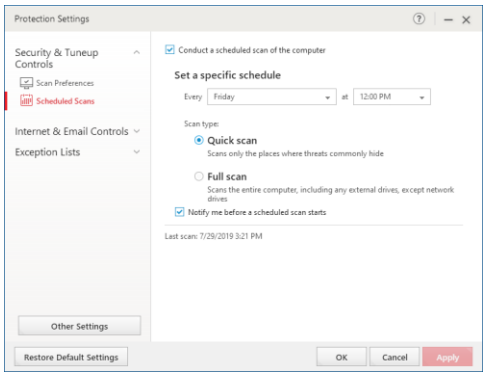



**Figure 144. Security & Tuneup Controls > Scheduled Scans**

2. Choose among the following options:

   - **Conduct a scheduled scan of the computer.** This is enabled by default. "Friday at 12:00 PM" is chosen by default as the day and time to conduct the scheduled scan. Use the popup menus to change the day and time the scheduled scan will be conducted.

**TIP:** **Scheduled scans are best conducted when the computer is on but not in use, as they take up a portion of Memory, CPU, and Disk processes.**

   - **Scan Type. Quick Scan** is selected by default.
     - Select **Quick Scan** to scan only the places where threats commonly hide.
     - Select **Full Scan** to scan the entire computer, including any external drives, except network drives.
     - Notify me before a schedule scan starts. Selected by default.

3. Click **Apply** to apply any changes, then **OK** to close the **Protection Settings** window.

# Device: Security Settings: Internet & Email Controls > Web Threats

**To modify the Internet & Email Controls > Web Threats settings:**

1. Click **Internet & Email Controls.** The **Web Threats** panel appears by default.

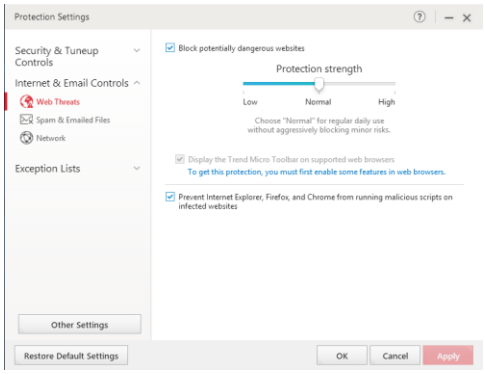



**Figure 145. Internet & Email Controls > Web Threats**

2. **Block potentially dangerous websites** is checked by default.
3. For **Protection strength**, use the slider to select the strength. More aggressive blocking blocks more websites, some of which you may not wish to be blocked.
   - **Low** - Choose “Low” to block only websites confirmed as fraudulent or dangerous.
   - **Normal** - Choose “Normal for regular daily use without aggressively blocking minor risks. This is the default setting.
   - **High** - Choose “High” to block threats in sites that show *any* signs of fraud or malicious software.
4. **Display the Trend Micro Toolbar on supported web browsers.** This enables Antivirus+ to rate links on webpages or mouseovers for malicious URLs and their accompanying payload for Internet Explorer, Mozilla Firefox, and Google Chrome. This is enabled by default.

**Note:** **To get this protection you must first install Trend Micro Toolbar in your default web browser. See Install Trend Micro Toolbar for Google Chrome, Mozilla Firefox, or Internet Explorer in Chapter 2 for details. Or go to our Trend Micro Toolbar Help Center for instructions.**

5. **Prevent Internet Explorer, Firefox, and Chrome from running malicious scripts on infected websites.** This is enabled by default.
6. Click **Apply** to apply your changes, then **OK** to close the **Web Threats** window.

# Device: Security Settings: Internet & Email Controls > Spam & Emailed Files

You can block spam from your Microsoft Outlook email client.

**Note:** **Fraud Buster also blocks spam and phishing emails with dangerous files and links in Gmail and Outlook webmail. See Antispam: Enable Fraud Buster for Gmail and Outlook Webmail following for details.**

**To modify the Internet & Email Controls > Spam & Emailed Files setting:**

1. Click **Internet & Email Controls > Spam & Emailed Files** to open the panel. The panel opens with the settings unchecked by default.

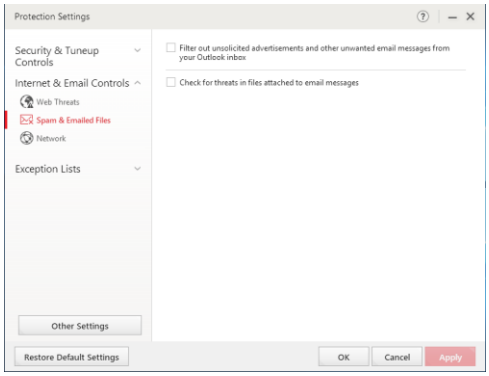



**Figure 146. Internet & Email Controls > Spam & Emailed Files**

- **Filter out unsolicited advertisements and other unwanted email messages from your Outlook inbox.** This is unchecked by default. Check this if you wish to stop spam and other unsought messages.
- **Check for threats in files attached to email messages**. This is unchecked by default. Check this to scan all email messages for malicious attachments and remove them.

2. Click **Apply** to apply any changes, then **OK** to close the **Protection Settings** window.
3. Trend Micro Anti-Spam (TMAS) support per OS Platform and Outlook version is given in the table below. Apart from Outlook 2003, the Data Theft Prevention feature also applies to these platforms and versions of Outlook.

**Table 8. TMAS OS Platform and Mail Client Support**

| OS Platform | Mail Client |
|---|---|
| Windows 7, 8.1, 10 (32 and 64 bit) | Outlook 2003 (32bit), 2007 (32bit), 2010 (32bit, 64bit), 2013 (32bit, 64bit), 2016 (32bit, 64bit) |

**To modify the Antispam Settings in the Microsoft Outlook Application:**

Once you've enabled the Antispam features for Outlook, you can modify the settings to your liking.

1. In the Microsoft Outlook application, select **Add Ins** in the **Main Outlook Toolbar.** The **Add-ins** panel appears.

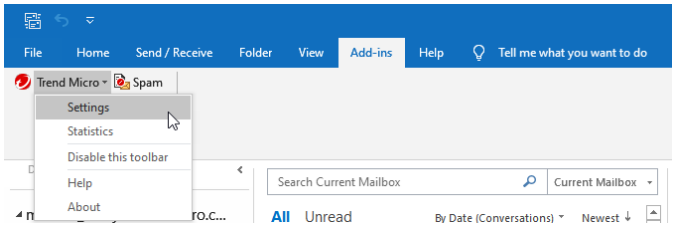



**Figure 147. Microsoft Outlook > Trend Micro Antispam Toolbar**

2. To mark an email as spam and add it to the **Spam** folder in Outlook, select the email in your email list, then click the **Spam** button.
3. See **Settings** below to set your settings.
4. Select **Statistics** to view statistics about the number of messages processed, spam messages deleted, spam messages you reported, and legitimate messages misidentified as spam.
5. You can also **Reset** the **Statistics** window to Zero by clicking **Reset**.

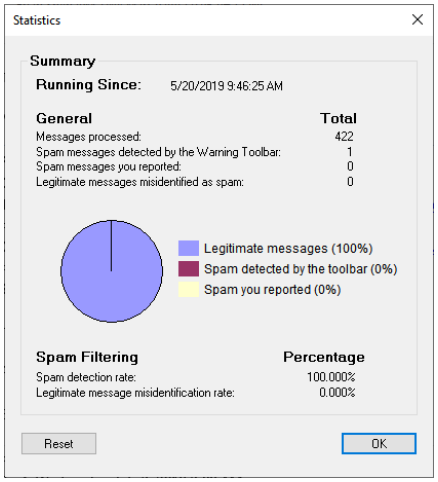



**Figure 148. Spam Statistics**

6. Select **Disable this toolbar** to disable it.
7. Select **Help** to get help using the **Antispam Toolbar.**
8. Select **About** to view the toolbar version.
9. Select **Settings** to configure the settings for the **Antispam Toolbar**. The **Settings** dialog box appears, with the **Spam Filter** tab selected by default.

### Spam Filter

**Spam Email Filter Strength** is set to **Medium** filtering by default.

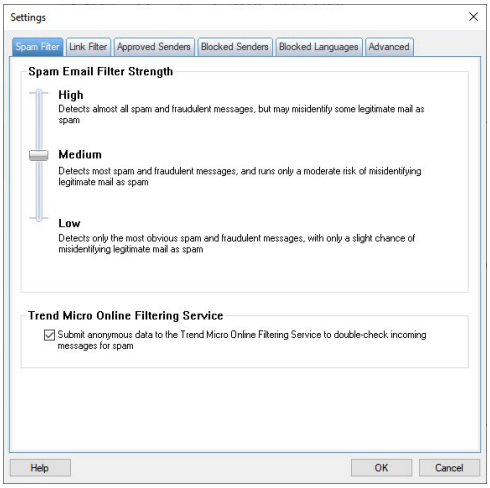



**Figure 149. Spam Filter**

1. Choose the **Spam Email Filter Strength** you want:
   - **High**. Detects almost all spam and fraudulent messages but may misidentify some legitimate email as spam.
   - **Medium**. Detects most spam and fraudulent messages and runs only a moderate risk of misidentifying legitimate email as spam.
   - **Low**. Detects only the most obvious spam and fraudulent messages, with only a slight chance of identifying legitimate email as spam.
2. **Trend Micro Online Filtering Service.** Submit anonymous data to the Trend Micro Online Filtering Service to double-check incoming messages for spam.
3. Click **OK** to save any changes.

### Link Filter

1. Click the **Link Filter** tab to edit the setting. The **Link Filter** screen appears.

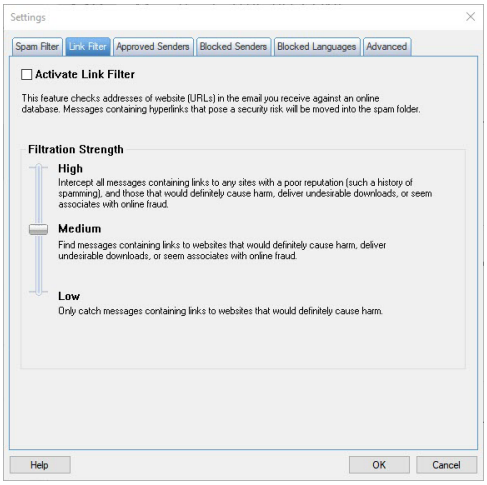



**Figure 150. Link Filter**

2. **Activate Link Filter.** This is turned off by default. Check this checkbox to activate the link filter. This filter checks addresses of website URLS in the email you receive against an online database. Messages containing hyperlinks that pose a security risk will be moved into the spam folder

3. **Filter Strength.** Choose the Filter Strength you want:

   - **High.** Intercept all messages containing links to any site with a poor reputation (such as a history of spamming, and all those that would definitely cause harm, deliver undesirable downloads, or seem associated with online fraud.
   - **Medium.** Find messages containing links to websites that would definitely cause harm, deliver undesirable downloads, or seem associated with online fraud.
   - **Low.** Only catch messages containing links to websites that would definitely cause harm.

4. Click **OK** to save any changes.

## Approved Senders

1. Click the **Approved Senders** tab to add approved senders. The **Approved Senders** screen appears.

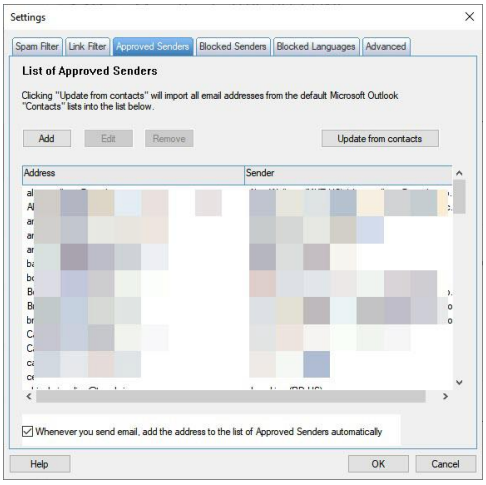



**Figure 151. Approved Senders**

2. **Update from Contacts**. Clicking “Update from contacts” will import all email addresses from the default Microsoft Outlook “Contacts” list into the list in the window.

3. **Add**. Click **Add** to add individual contacts. The **Add approved senders** dialog box appears.

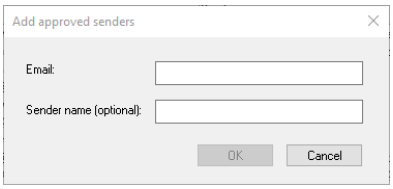



**Figure 152. Add Approved Senders**

4. Type in the email address of the person you wish to add to the list of **Approved Senders**.

5. Type in the sender’s name (optional).

6. Click **OK** in the dialog box to save the email address/contact in the list of **Approved Senders**.

7. Select an email address and click **Edit** to edit an email entry. A dialog appears to let you edit the entry; click **OK** to save your changes or **Cancel** to cancel the edit.

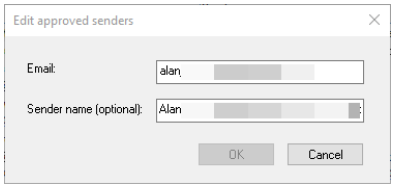



**Figure 153. Edit Approved Senders**

8. Select an email address and click **Remove** to remove an email entry. A dialog appears to let you remove the entry; click **OK** to remove it or **Cancel** to retain it.

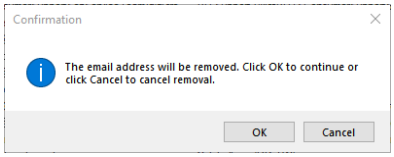



**Figure 154. Confirm Removal**

9. Check/uncheck the checkbox **Whenever you send email, add the address to the list of Approved Senders automatically.**
10. Click **OK** in the **Approved Senders** window to save your changes.

## Blocked Senders

1. Click the **Blocked Senders** tab to add **Blocked Senders** to the list. The **Blocked Senders** screen appears.

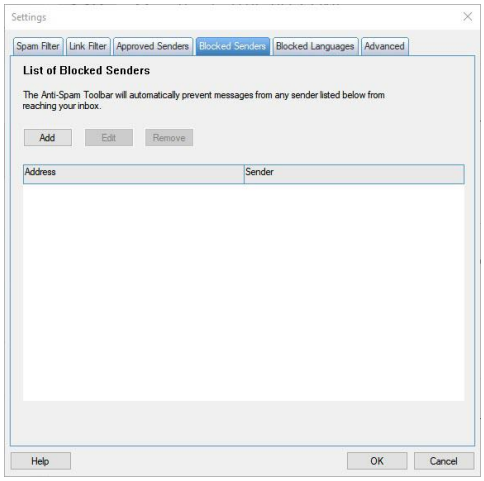



**Figure 155. Blocked Senders**

2. **Add, Edit,** or **Remove Blocked Senders** to the list in the same way you did for **Approved Senders.**
3. Click **OK** to save your changes.

## Blocked Languages

1. Click the **Blocked Languages** tab to edit the settings. The Blocked Languages screen appears.

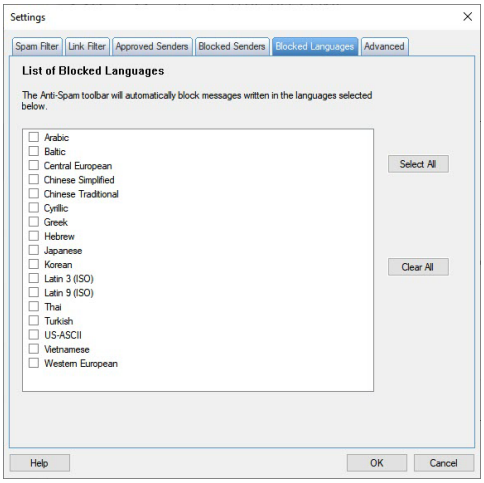



**Figure 156. Blocked Languages**

2. Individually check the languages you wish to block or **Select All** or **Clear All**.
3. Click **Ok** to save your changes.

## Advanced

1. Select the **Advanced** tab to open the **Advanced** screen.

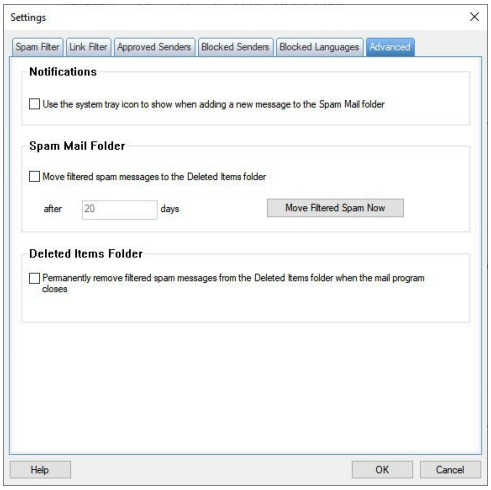



**Figure 157. Advanced**

- **Notifications**. Check this checkbox to use the system tray icon to show when adding a new message to the **Spam Mail** folder.

- **Spam Mail Folder.** Check this checkbox to move filtered spam messages to the **Deleted Items** folder. Options include:
    a. **Move after XX days.** Add the number of days you wish to hold messages before they're moved to the **Deleted Items** folder.
    b. **Move Filter Spam Now.** Click this button to move all **Filtered Spam Now** to the **Deleted Items** folder now.
- **Deleted Items Folder.** Check this checkbox to permanently remove filtered spam messages from the Deleted Items folder when the mail program closes.

2. Click **OK** to save your changes.

## Device: Security Settings: Internet & Email Controls: Network > Firewall Booster | Wi-Fi Protection

**To modify the Wi-Fi Protection Settings:**

1. Click the **Settings** tool in the **Console**. The **Protection Settings** screen appears, with **Security & Tuneup Controls > Scan Preferences** selected by default.
2. Click **Internet & Email Controls > Network** in the **Command** menu. The **Network** screen appears.

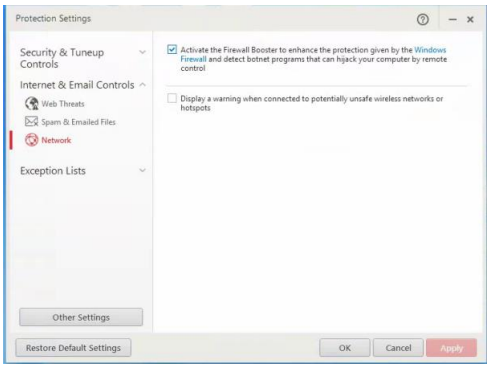



**Figure 158. Internet & Email Controls > Network**

3. **Activate the Firewall Booster** is checked by default. This enhances the protection given by the Windows Firewall and detects botnet programs that can hijack your computer by remote control.
4. **Display a warning when connected to potentially unsafe wireless networks or hotspots**. This is disabled by default. Check this to enable the feature.
5. Click **OK** to save your changes.

**Note:** **The Exception List for Wi-Fi Protection allows users to add unprotected home networks to an exception list, so that users are not subject to frequent warnings for networks they know to be safe. See the Exception Lists section below for more details.**

# Exception Lists: Programs/Folders

**To add items to Exception Lists Programs/Folders:**

Trend Micro Security lets you add programs, folders, or websites to exception lists so that scans will ignore them. Adding programs or folders to exception lists can increase performance during scans, while adding frequently-accessed websites can prevent unwanted blockage. Users are advised to use exception lists wisely, as it may open computers up to more threats.

1. To add items to exception lists, click **Exception Lists**. **Programs/folders** appears by default.

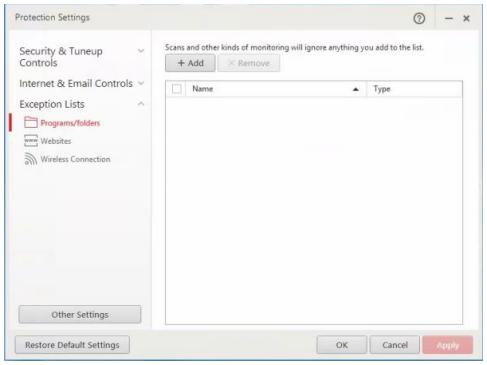



**Figure 159. Exception Lists > Programs/folders**

2. Click **+Add** to add a program or folder to the exception list. A dialog appears, letting you **Add an Item.**

**Figure 160. Add an Item**

3. Click **Browse** to browse to the file or folder you wish to add. An **Open** dialog appears.

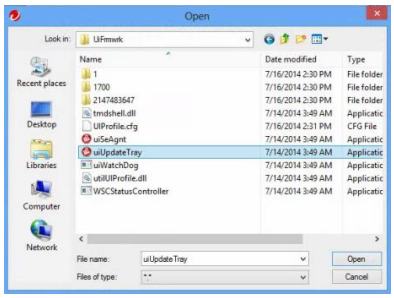



**Figure 161. Open Dialog**

4. Select the item you wish to add, then click **Open**. This adds the item to the **Add an Item** dialog.

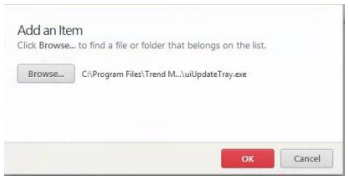



**Figure 162. Add an Item (item added)**

5. Click **OK** in the **Add an Item** dialog. The item is added to the exception list.

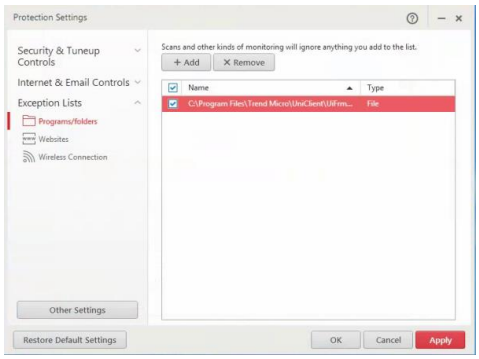



**Figure 163. Item Added to Exception List**

6. To remove an item, check it, and then click the **X Remove** button.

7. Click **Apply** to save any changes, then **OK** to close the Trend Micro Security Console.

# Exception Lists: Websites

**To add websites to an exception list:**

1. In a similar way, to add or remove a website from its exception list, click **Exception Lists > Websites** in the **Command Menu**. The **Websites** exception list appears.

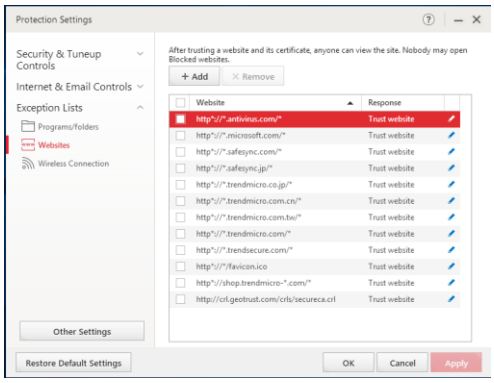



**Figure 164. Exception Lists > Websites**

2. Click **Add** to add a website. A dialog appears, letting you **Add** or **Edit an Item.**

3. Choose among the following options:

   a. Type in the URL you wish to add in the edit field.

**Figure 165. Add or Edit an Item**

   b. Or select Import addresses (URLs) from your Internet Explorer “Favorites”.

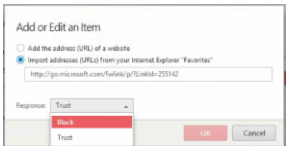



**Figure 166. Import URLs from IE**

   c. Choose **Block** or **Trust** from the **Response** pop-up (for either option).

   d. Click **OK** to save the option.

4. Click **Apply** to save your changes, then **OK** again to close the Trend Micro Security Console.

# Exception Lists: Wireless Connection

Trend Micro Security allows you to add access points to the **Wireless Connections Exception List** that Trend Micro Security may consider risky or dangerous. Wi-Fi hotspots added to the list are considered trusted access points.

**To add and remove a Wireless connection to the Exception List:**

1. When you attempt to log onto an access point, Trend Micro Security may give you a pop-up warning that the network connection is risky or dangerous.

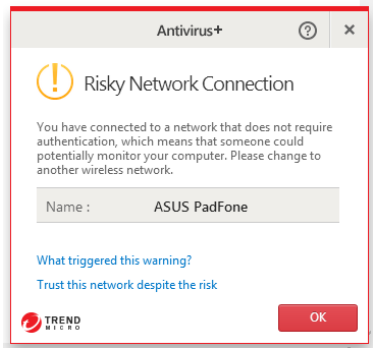



**Figure 167. Risky Network Connection**

2. If you know this access point probably isn't risky, you may wish to add this network to the Wireless Connections Exception List. To do so, simply click **Trust this network despite the risk** and the site will be added to the list.
3. Later, you may wish to delete this from the Exception List. To do so, click the **Settings** tool to open the **Protection Settings** screen. The **Virus & Spyware Controls** screen opens by default.
4. Click **Exception Lists > Wireless connection** in the Command menu. The **Exception** List for **Wireless Connection** appears.

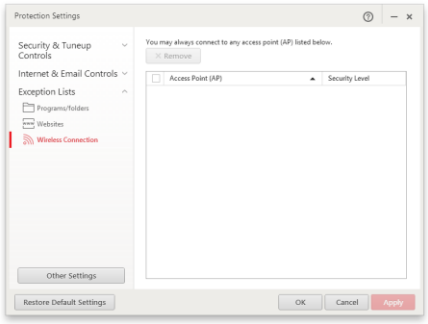



**Figure 168. Exception Lists > Wireless Connection**

5. Select the access point in the list and click **Remove**. Trend Micro Security deletes it from the list.
6. Click **Apply** to save your changes.

# Other Settings: System Startup

By default, Trend Micro Security chooses the optimal settings when starting your computer. You can change these settings.

**To modify Other Settings > System Startup:**

1. Click **Other Settings** in the Command Menu. The **System Startup** screen appears by default, with **Balanced Protection (Recommended)** chosen by default.

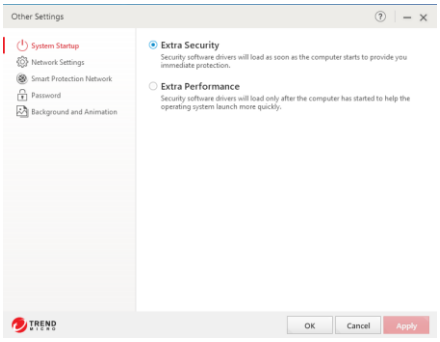



**Figure 169. Other Settings > System Startup**

2. Select between the following options:

- **Extra Security** – This is the default option. Security software drivers will load as soon as the computer starts, which makes the operating system launch more slowly.
- **Extra Performance** – Security software drivers will load only after the computer has started to help the operating system launch more quickly.

3. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.
4. Restart the computer to apply the changes to your system.

# Other Settings: Network Settings

**To modify Other Settings > Network Settings:**

1. Click **Other Settings > Network Settings** in the Command Menu. **Network Settings** appears, with **Use a proxy server to connect to the Internet** and **Use the proxy settings saved on your computer** chosen by default.

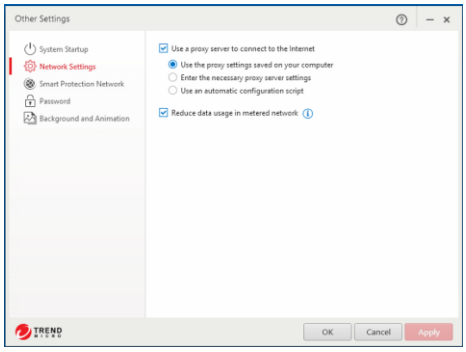



**Figure 170. Other Settings > Proxy Settings**

2. **Reduce data usage in metered network** is also selected by default. The frequency of maintenance software updates will be less than on a non-metered network.
3. Select **Enter the necessary proxy server settings** to manually enter a proxy server's name, port, and credentials (if required).

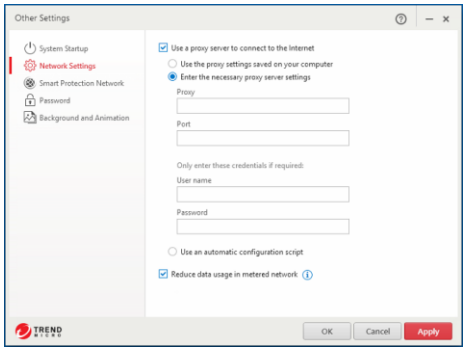



**Figure 171. Other Settings > Proxy Settings > Enter Settings**

4. Or select **Use an automatic configuration script** and enter the script in the **Address** field provided.

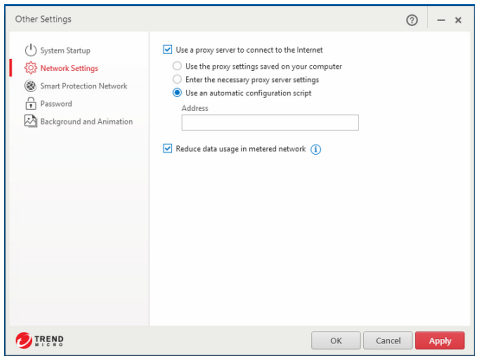



**Figure 172. Other Settings > Automatic Configuration Script**

5. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

# Other Settings: Smart Protection Network

Trend Micro Security can provide feedback to the Smart Protection Network (SPN), to automatically correlate and analyze information about threats found on your computer (and millions of others), for better protection. By opting into the SPN feedback process, you improve yours and others' threat protection, since threats sent from your computer are immediately added to the threat analysis/detection/prevention process, but the choice is yours to opt in or out. You can also opt into sharing computer performance information with Trend Micro, to help yours and others' computers work better.

**To share/not share feedback with the Smart Protection Network:**

1. Select **Other Settings > Smart Protection Network** from the **Command Menu.** The threat information feedback panel appears.

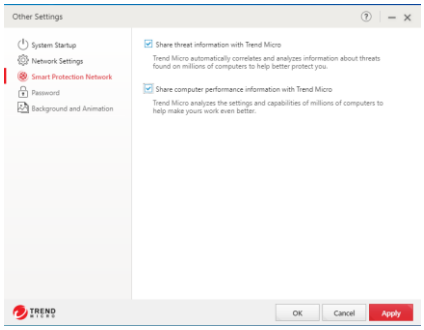



**Figure 173. Other Settings > Smart Protection Network**

2. Check/Uncheck **Share threat information with Trend Micro** to opt in or out of the feedback process. (This will be checked or unchecked depending upon the choice you made to participate or not participate when you installed Trend Micro Security.)

3. Check/Uncheck **Share computer performance information with Trend Micro.** Trend Micro analyzes the settings and capabilities of millions of computers to help yours work even better.
4. Click **Apply** to save your changes, then **OK** to close the **Protection Settings** window.

# Other Settings: Password

**To add or change your password:**

The Trend Micro Security Family, which includes Antivirus+ (AV+), allows you to add a password to protect your overall program settings, so only those who know the password can make changes. For Trend Micro Security Internet Security (IS) and Maximum Security (MS), the password enables other functions, such as **Parental Controls** in IS and MS and **Trend Micro Vault** in MS. See the following two chapters for details.

1. Select **Other Settings > Password** from the Command Menu. The **Password** screen appears.

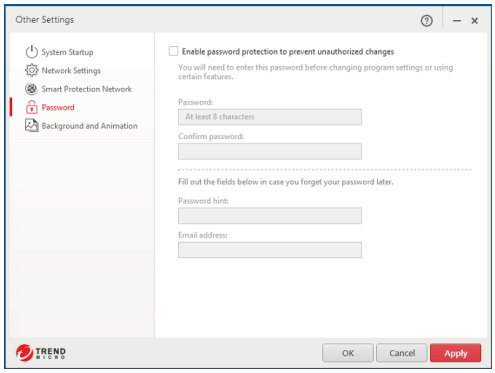



**Figure 174. Other Settings > Password**

2. Check **Enable password protection to prevent unauthorized changes**.
3. Enter your email address, a password, and the password again to confirm it. Trend Micro Security gives you feedback on your password strength.
4. Fill out the **Password Hint** and **Email Address** fields in case you forget your password later.
5. Click **Apply** to save the password changes, then **OK** to close the **Protection Setting** window.

# Other Settings: Background and Animation

Trend Micro Security allows you to change the background picture and animation effects on the **Trend Micro Security Console.** You can use backgrounds provided by Trend Micro, or customize the background using your own pictures. You can also show animation effects on the main Console.

**To change your Trend Micro Security interface:**

1. In **Other Settings**, select the **Background and Animation** menu item. The **Background Editor** appears.

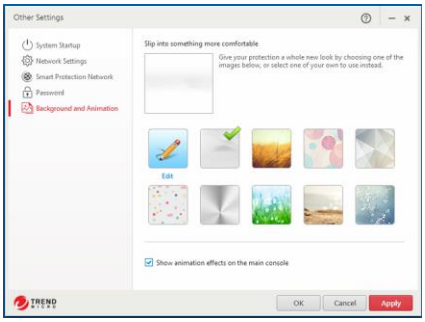



**Figure 175. Background Editor**

2. Select any background picture provided and click **Apply** to save the new background or add a picture from your computer.

3. For the second option, click the **Edit** button to edit your user interface. The **Select a Picture** dialog displays.

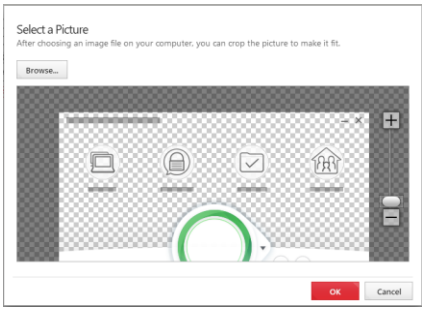



**Figure 176. Select a Picture**

4. Click **Browse** to select a picture, then navigate to a folder containing your pictures.

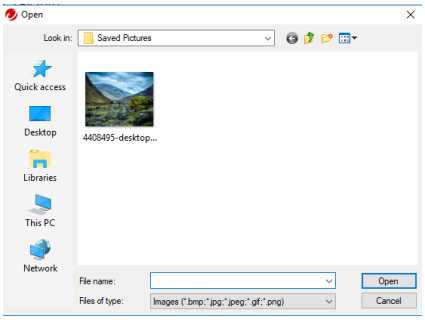



**Figure 177. Browse to Picture**

5. Select your picture and click **Open**. The picture is loaded into the editor.

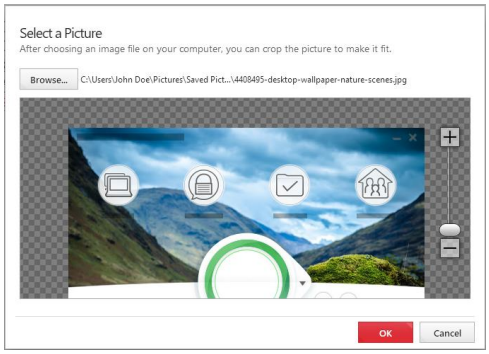



**Figure 178. Sizing**

6. Use the **Sizing** tool to make your image larger or smaller. Click the (**+**) or (**-**), or drag the slider.
7. When you're done, click **OK** to close the editor.
8. Click **Apply** to save your UI change, the **OK** to close the **Background Picture** tab.
9. Navigate to the main Console screen. Your new picture appears in the background.

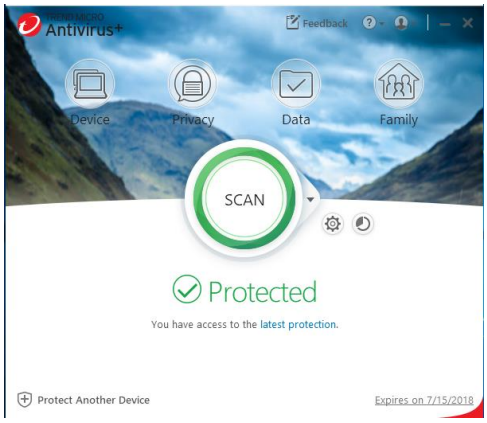



**Figure 179. Trend Micro Security Console with New Skin**

10. You can return to the classic Trend Micro Security background at any time by clicking its icon in the editor and clicking **Apply,** then **OK**; then return to the main Console screen.

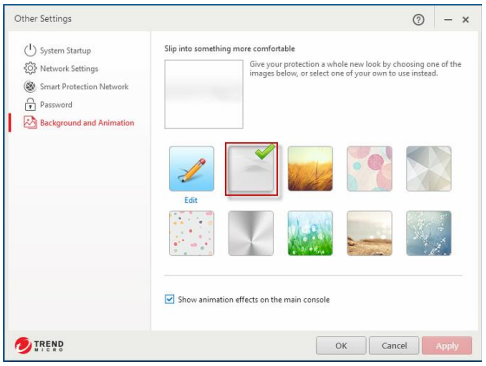



**Figure 180. Classic Trend Micro Security Background**

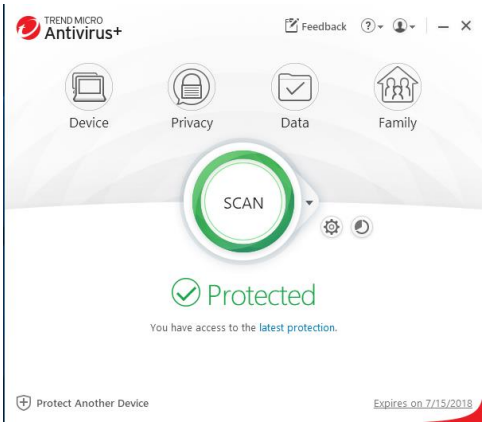



**Figure 181. Trend Micro Security Console**

11. If you wish, you may also uncheck the checkbox **Show animation effects on the main console**. This reduces the animation effects in the four functional icons of **Device, Privacy, Data,** and **Family.**

# Device: Mute Mode

All editions of Trend Micro Security now provide a **Mute Mode** to temporarily stop non-critical notifications while you are doing an important task. This can also be applied while gaming.

**To configure Mute Mote:**

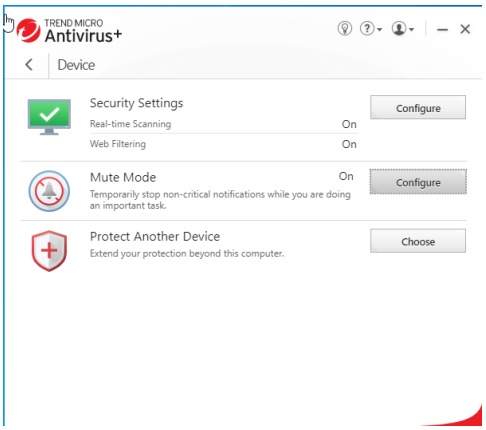



**Figure 182. Device > Mute Mode > Configure**

1. Click **Device > Mute Mode > Configure**. The **Mute Mode Introduction** screen appears.

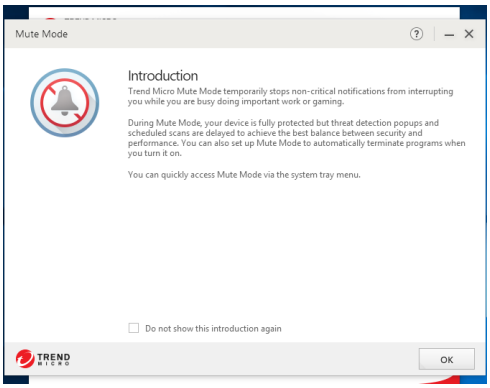



**Figure 183. Mute Mode Introduction**

2. Click **OK** to close the **Introduction**. The **Mute Mode Configure** screen appears, with the feature toggled **Off** by default.

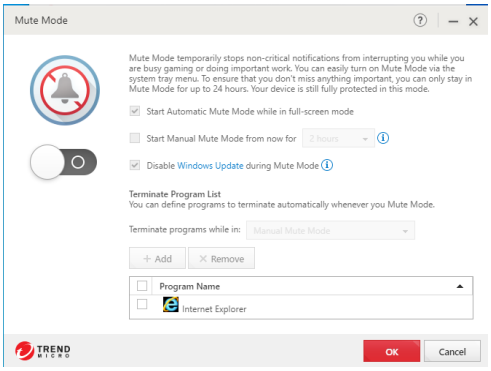



**Figure 184. Mute Mode Off**

3. Toggle **Mute Mode On** to set the settings:
   - **Start Automatic Mute Mode while in full-screen mode.** This is enabled by default.
   - **Start Manual Mute Mode from now for [X hours]**. Check the checkbox, then select your choice in the drop-down menu to turn off Mute Mode after 1 to 24 hours.
   - **Disable Windows Update in Mute Mode**. This is enabled by default. Check the checkbox to disable Windows Update for as long as **Mute Mode** is active. (Disabling Windows Update for a long time may expose your system to security threats.)
4. **Terminate Program List**. You can define the programs you want to automatically terminate whenever you enable Mute Mode.
5. **Terminate Programs while in** [dropdown menu], then choose the option you prefer by selecting it in the menu.
   - **Automatic Mute Mode**
   - **Manual Mute Mode**
   - **Automatic and Manual Mute Modes**
6. Click the **+ Add** button to add program(s) you would like to terminate in **Mute Mode.** The **Mute Mode** program selection dialog appears.

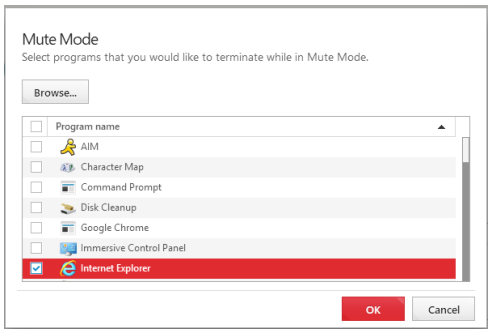



**Figure 185. Mute Mode Program Selection List**

7. Select the program(s) you wish to terminate in **Mute Mode**, then click **OK**. The program(s) you wish to terminate are added to the list.

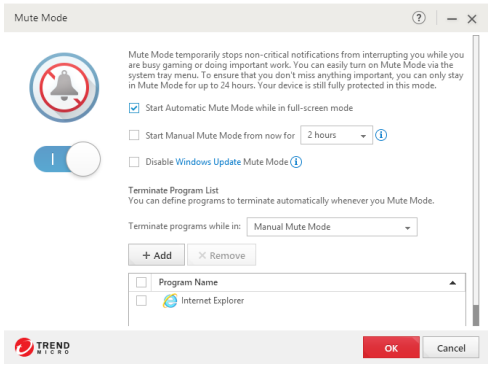



**Figure 186. Mute Mode Program Selected List**

8. Click **OK** to complete the setup. **Mute Mode** shows as **On** in the **Device** window.

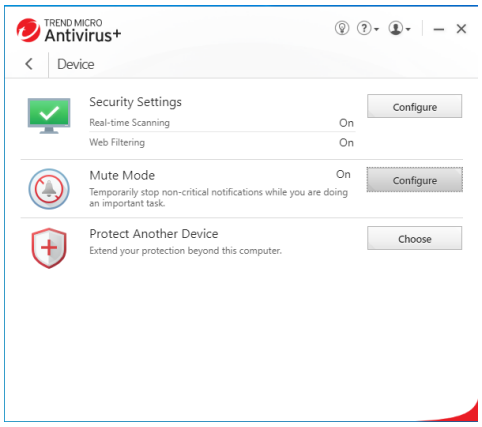



**Figure 187. Mute Mode On**

9. If you wish, click **Configure** again, then toggle **Mute Mode** to **Off** to turn it off before the allotted time has expired.

# Device: Protect Another Device

Trend Micro Antivirus+ Security provides a subscription for one Windows device, but also lets you switch your protection to another Windows device. When you do so, you lose protection on the first device. Go to **Protect Another Device** for more details.

# Privacy: Social Networking Protection

All editions of Trend Micro Security provide Social Networking Protection to keep you safe from security risks when visiting the most popular social networking sites such as Facebook, Twitter, Google+, LinkedIn, Mixi, MySpace, Pinterest, and Weibo. In Facebook, you can also warn a friend when a link is dangerous. The function is turned on by default in Trend Micro Antivirus+, Internet Security, and Maximum Security, automatically activating the Trend Micro Toolbar.

**To use Social Networking Protection:**

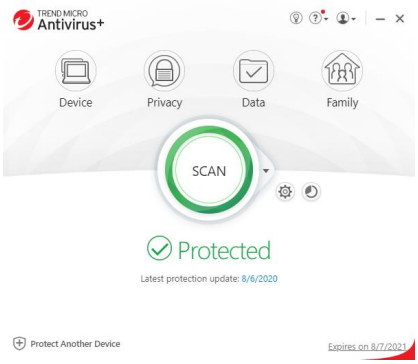



**Figure 188. Console > Privacy**

1. To configure **Social Networking Protection**, click **Privacy** in the Console. The **Privacy** screen appears, with the **Social Networking Protection** panel at the top.

**Figure 189. Social Networking Protection**

2. Click **Configure**. The **Social Networking Protection** toggle screen appears.

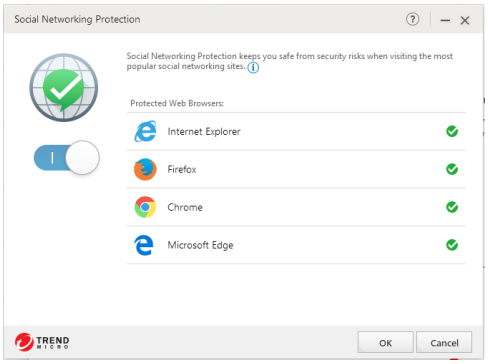



**Figure 190. Social Networking Protection On**

3. **Social Networking Protection** is turned **On** by default and the browser(s) installed on your system are shown. Trend Micro Security protects Internet Explorer, Firefox, Chrome, and Edge on the PC. If you wish, click the slider from **On** to **Off** to disable the function. Trend Micro does not recommend this.

4. Open your browser, select the **Trend Micro Toolbar**, and note that **Rate links on web pages** is selected by default.

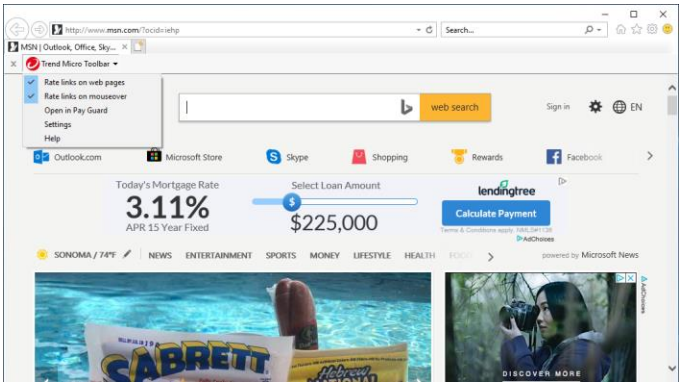



**Figure 191. Rate Links on Web Pages**

5. Select **Rate links on mouseover** to enable the feature. Now, when you mouse-over a link in search results, Trend Micro Security will scan it in real-time and provide you with a rating and details about it.

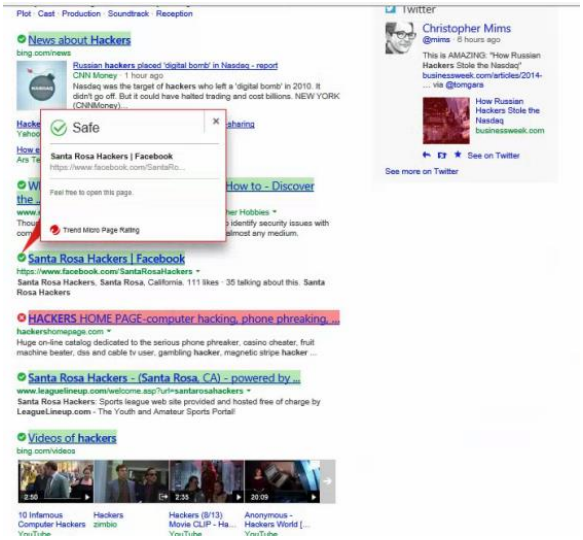



**Figure 192. Safe Trend Micro Page Rating**

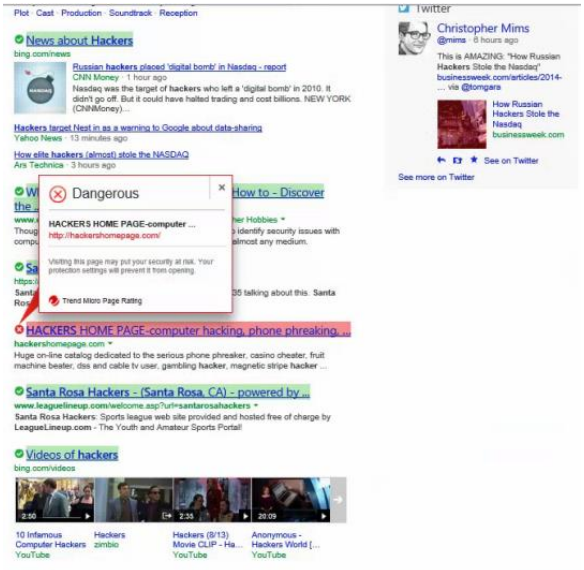



**Figure 193. Dangerous Trend Micro Page Rating**

6. Simply position your mouse over the checkmark to view details about the rating.
7. If you click on a bad link, you'll be blocked.

**Figure 194. Dangerous Page**

8. You can still open the page by clicking **Still want to open this page, despite the risk?** Trend Micro doesn't recommend this.

9. The same link ratings and mouse-over functions are available from within supported social networking sites. Note too, that when a URL posted on Facebook is rated as dangerous by Trend Micro Security, you can warn your friend about it.

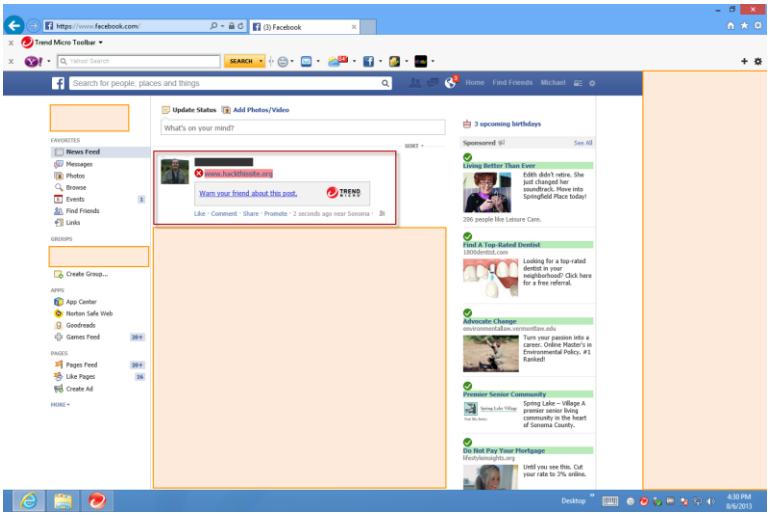



**Figure 195. Dangerous URL on Facebook Detected by Trend Micro Security**

10. Below the dangerous URL, click the link **Warn your friend about this post.** Trend Micro Security adds the warning to the comment field.

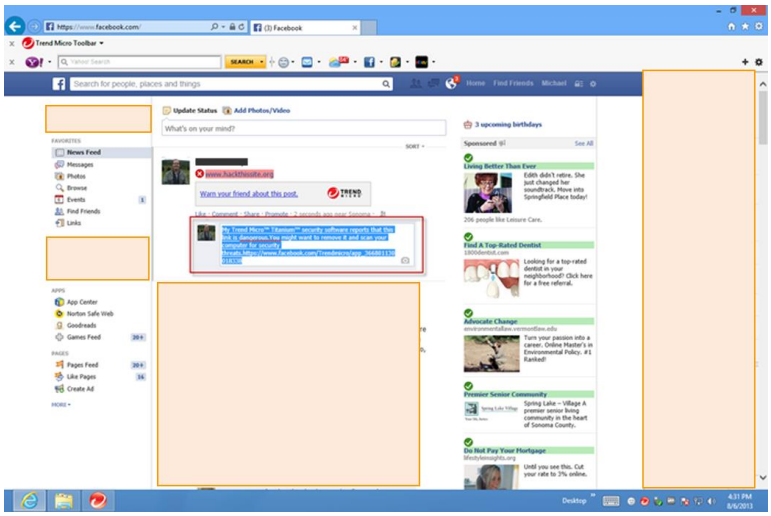


**Figure 196. Warn a Friend About the Dangerous URL**

11. Click **Enter** to post the warning. Trend Micro Security posts the warning along with a **Welcome** link from Trend Micro. The user is advised to remove the dangerous link and to scan their computer for security threats.

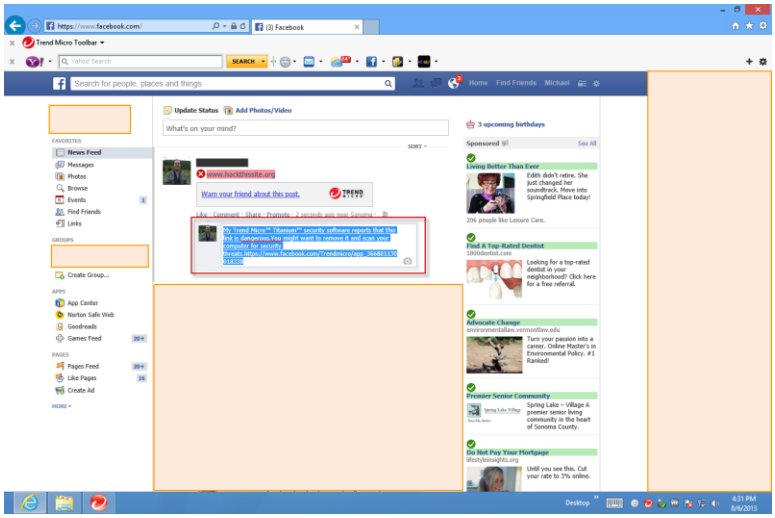


**Figure 197. Dangerous URL Warning Posted on Facebook**

# Privacy: Pay Guard

All editions of Trend Micro Security provide **Pay Guard**, which helps keep you safe from security risks when banking or shopping online with Chrome, Firefox, Edge, or Internet Explorer. When you open **Pay Guard**, its powerful protection features are applied to your default browser automatically.

**Pay Guard** protects all the data in your financial transactions, including credit card information and personal data. With **Pay Guard**, all the extensions in your default browser

are turned off. Security-related extensions, such as **Trend Micro Toolbar** or **Password Manager**, may be added later, if you choose. The next time you use Pay Guard, they'll also be loaded.

**To open Pay Guard:**

1. Double-click the **Pay Guard** shortcut on your Windows desktop.

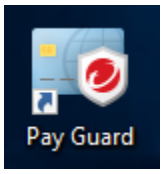



**Figure 198. Pay Guard Shortcut**

2. **Trend Micro Pay Guard** opens, using the protected version of your default browser.

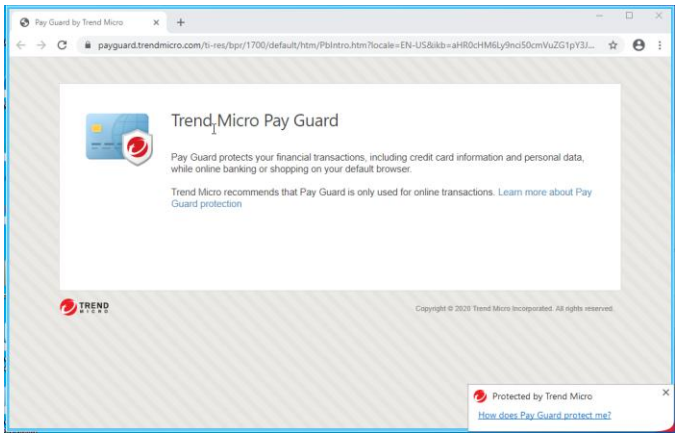



**Figure 199. Trend Micro Pay Guard (Chrome Example)**

3. Browse to your bank or to a commercial site where you may wish to conduct financial transactions and sign in as you normally would. **Pay Guard** protects you against browser injections and other threats to your identity or security.

4. You may configure **Pay Guard** in the **Trend Micro Security Console** to automatically load when you go to a financial website. First, open the **Console**.

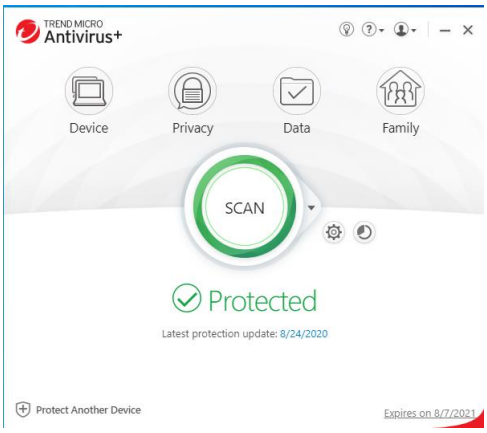



**Figure 200. Trend Micro Security Console**

5. Once the **Console** is open, click the **Privacy** icon. The **Privacy** screen appears, with the **Pay Guard** panel second in the list.

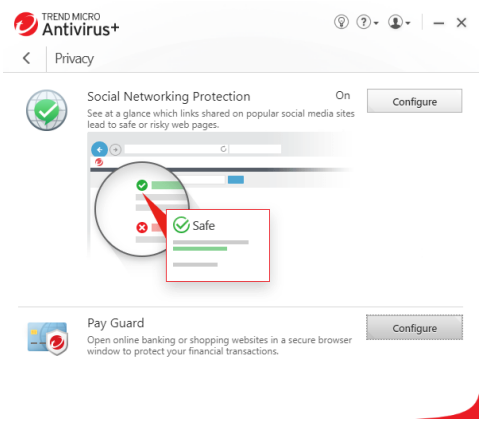



**Figure 201. Privacy > Pay Guard**

6. Click **Configure** in the **Pay Guard** panel. The **Introduction** screen appears.

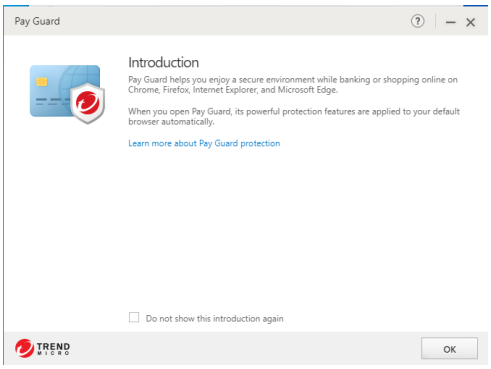



**Figure 202. Trend Micro Pay Guard Introduction**

7. Click **OK**, to close the **Introduction**. The **Pay Guard Configuration** screen appears.

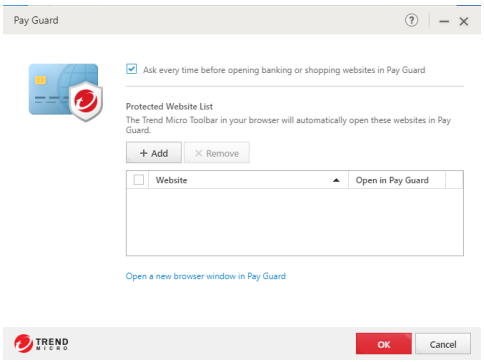



**Figure 203. Pay Guard Configuration**

8. Note that **Ask every time before opening banking or shopping websites in Pay Guard** is checked by default. Uncheck to disable the permission popup.

9. Click **(+) Add** to add a financial or commercial website to **Pay Guard.** A popup appears.

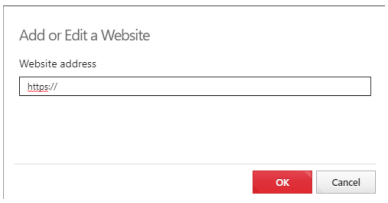



**Figure 204. Add or Edit a Website**

10. Type the URL of the website you wish to add. E.g., https://www.wellsfargo.com and click **OK.** The site is added to **Pay Guard.**

11. Launch your preferred browser and type the URL of the site you just added. **Pay Guard** launches and displays over your browser's page.

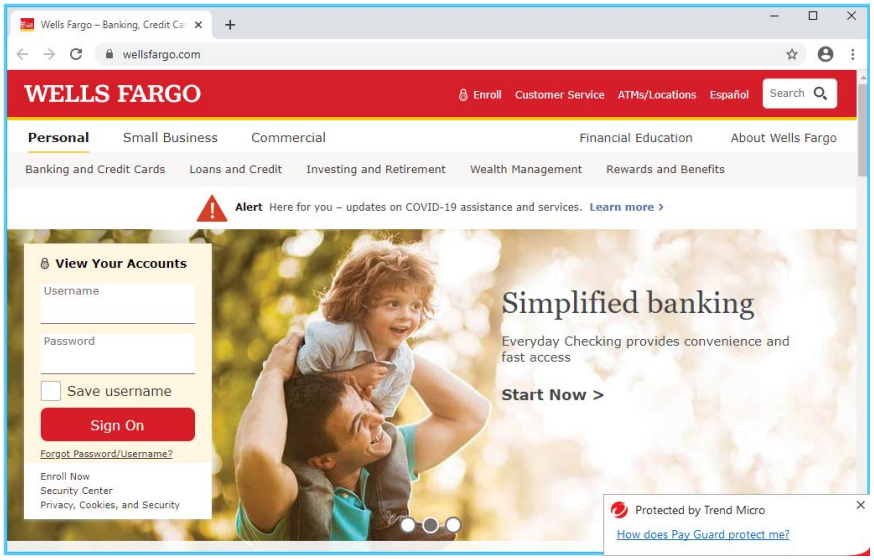



**Figure 205. Pay Guard -> Wells Fargo**

12. Log into your account using **Pay Guard**, knowing your transactions are kept secure.
13. Note that during first-time use, banks or other financial sites may ask you to verify your use of **Pay Guard**, so they recognize the browser.

# Data: Folder Shield

In the **Data** window, you can configure **Folder Shield** to your specifications.

**To configure Folder Shield:**

1. Open the **Trend Micro Security Console.**

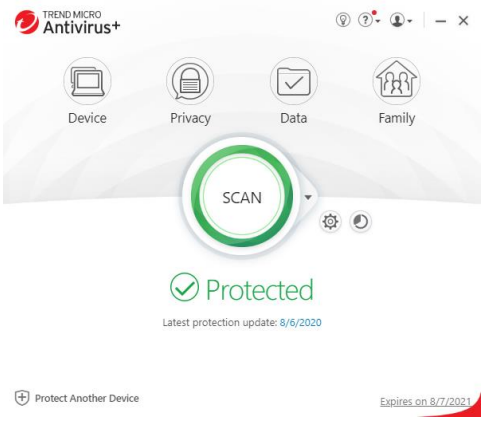



**Figure 206. Console > Data**

2. Click the **Data** icon. The **Data** screen appears.

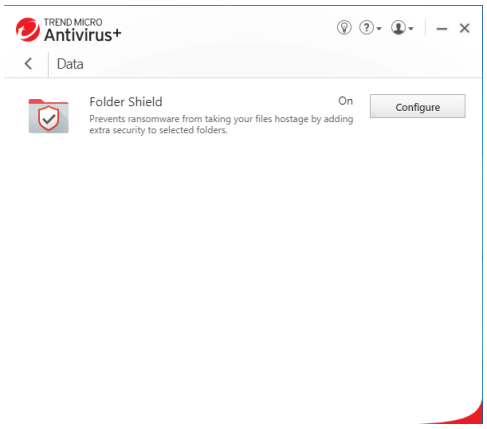



**Figure 207. Data | Folder Shield**

3. Click **Folder Shield > Configure** to configure the settings. The **Introduction** screen appears.

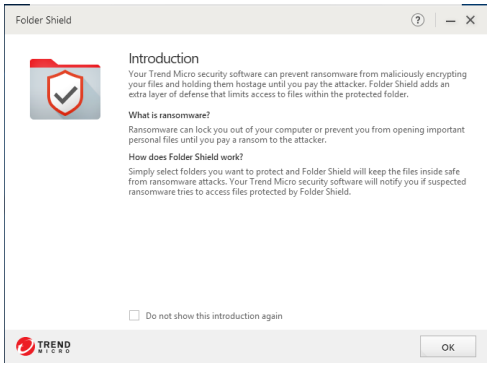



**Figure 208. Folder Shield Introduction**

4. Click **OK** to close the **Introduction**. The **Manage Folders** window appears.

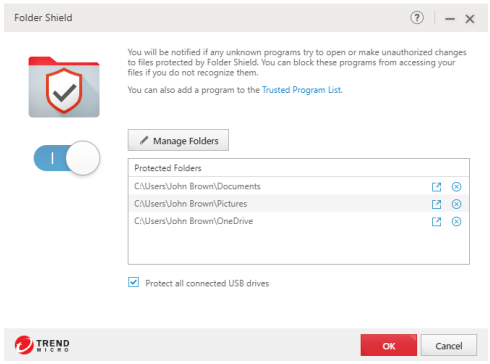



**Figure 209. Manage Folders**

5. Click the **X** button for any folders you wish to delete from the **Protect Folders** list.

6. Click the **Manage Folders** button to add folders to the **Protected Folders** list. A window appears letting you **Choose Folders to Protect.**

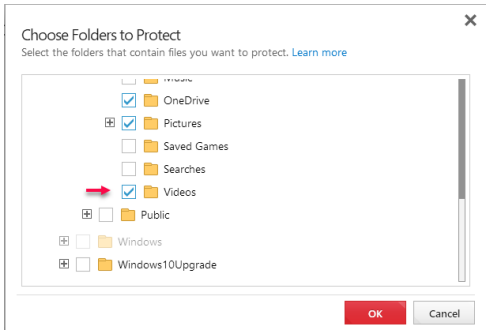



**Figure 210. Choose Folders to Protect**

7. Scroll up or down to choose the additional folder(s) in the **Folder Tree**. For example, you can select the main User's folder (this should be your name) to protect all folders for that User; or you may select additional individual folders for protection.

8. In this example, we choose **Videos**. Click **OK** to save your selection.

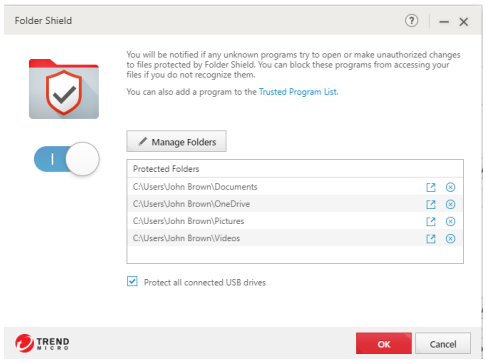



**Figure 211. Videos Added**

**Note:** **If you select the main user's folder, you may encounter additional warning popups under certain conditions. Don't worry! If you follow the rules given below for adding programs to the Trusted Program List, you'll still keep yourself safe.**

9. **Videos** now appears in the list. Click **OK** to close the window.

10. You can also click the link **Trusted Program List** to add a trusted program to a list of applications that can access protected folders. The **Trusted Program List** appears.

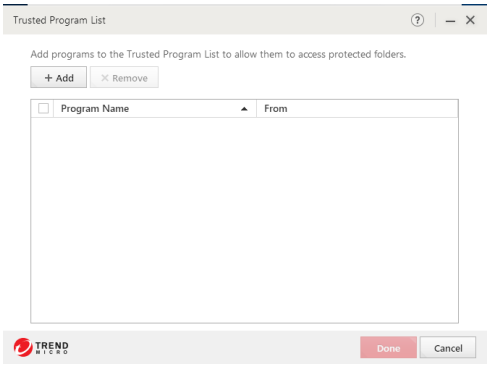



**Figure 212. Trusted Program List**

11. Click **+ Add** to add a program. A dialog appears, letting you **Add an Item** to the list.

**Figure 213. Add an Item**

12. Click **Browse**, then navigate to the **Program Files** folder on your computer.

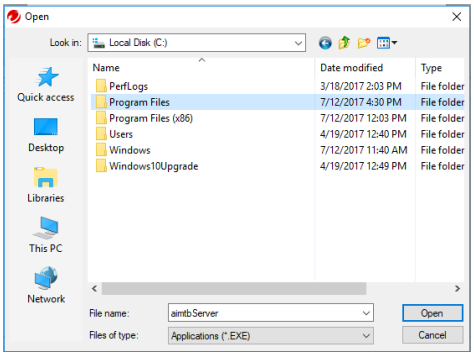



**Figure 214. Local Disk (C:) - Program Files**

13. In the **Program Files** folder, double-click folders to open them, until you locate the program you wish to add.

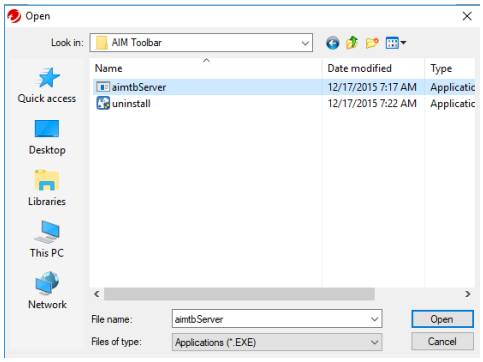



**Figure 215. AIM Toolbar**

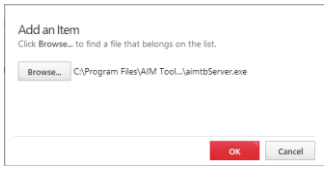



**Figure 216. Add an Item**

14. Select the **Application**, click **Open** to add it, then **Ok** to complete the process. The program appears in the **Trusted Program List.**

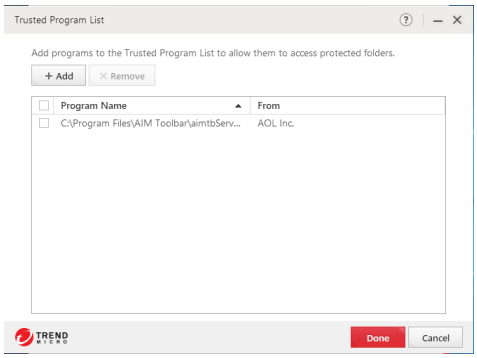



**Figure 217. Trusted Program List**

15. Click **Done**, then **OK** to close the **Folder Shield Configure** window. Your program is now added to the **Trusted Program List.**

## How Folder Shield Works

**Example 1:**

1. Now, what if a program that's not in Trend Micro's list of known good programs, such as encrypting ransomware, unexpectedly tries to change any files in your protected folder?
2. A popup will appear, asking if you want to **Block this program**. Because you also have the option to **Trust this program**, what should you do?

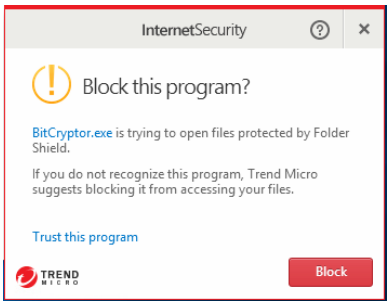



**Figure 218. Block this program?**

3. In a setting where you're just doing a search, or browsing a website, or watching a video and the pop-up appears, it's quite likely that malware or ransomware is trying to install, to maliciously change or encrypt your files. In this case, **Block** is the recommended action.
4. Note too, that even if the program trying to execute shows up under a familiar name—such as winword.exe (for Microsoft Word), excel.exe (for Microsoft Excel), or photoshop.exe (for Adobe Photoshop), *you should also click **Block**.*
5. Malware or encrypting ransomware can disguise itself under familiar program names and the unexpected nature of the event that triggered the popup is a clue that it's probably dangerous.

**Example 2:**

1. But what if you're just trying to open a file in your protected folder and the popup appears, asking you if you want to **Block this program**?

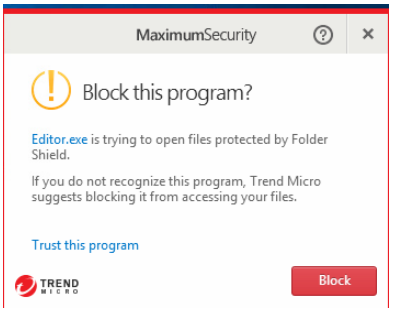



**Figure 219. Block this program?**

2. *Even in this case,* you should generally accept **Folder Shield's** judgment and click **Block** to stop the action.
3. So, when *should* you click **Trust this program?** Because trusted programs are automatically added to the **Trusted Program List,** potentially exposing you to risk, you should *only* click **Trust this program** under one or more of the following conditions:
    - If you remember downloading, installing, and using the program before.
    - If the program was downloaded from a reputable site, such as CNET's **Download.com**, which tests all software submitted to the site for malware before posting.
    - If you've done your research and have determined that the software has a known good reputation, as given on the official download page, along with frequently asked questions (or F-A-Qs) and/or a Support page, and does not appear in any websites that list malicious software.
    - If it's software that you have developed personally or internally for organizational purposes.
4. In this last instance, you may wish to file a reclassification case to Trend Micro Support, so the program will not be blocked by default by Folder Shield. Go here to find out how to do that: [Reclassification Requests]
5. Or go here for advice if you're worried you may be under attack by ransomware: [Ransomware Support]

6. After a few moments, if you don't click **Block**, **Folder Shield** will block the program anyway. The popup will change to **Programs Blocked**, and the **Trust this program** link will change to **More details…**

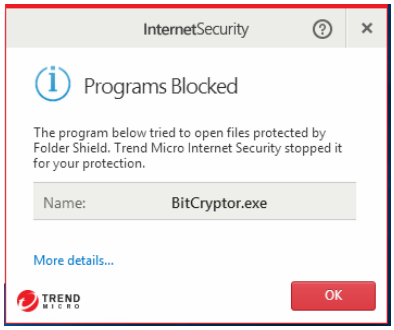



**Figure 220. Programs Blocked**

7. Click **More details…** to get more details on the programs blocked and the targeted file or files. The **Logs** window appears.

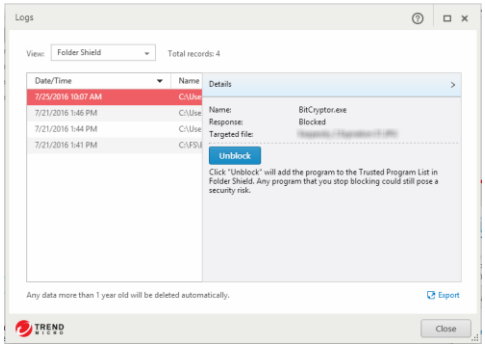



**Figure 221. Details**

8. The **Details** panel will show the **Name** of the program blocked, the **Response** taken, and the **Targeted file** or **files**.

9. If you click **Unblock**, the program will be added to the **Trusted Program** list. As mentioned, if you do this, you *could* open yourself to a security risk now or in the future.

10. Click the right-arrow to close the **Details** panel and view the **Folder Shield** log table, with the **Date/Time** of all incidents, the **Name** of the offending program, and the **Responses** shown in the table.

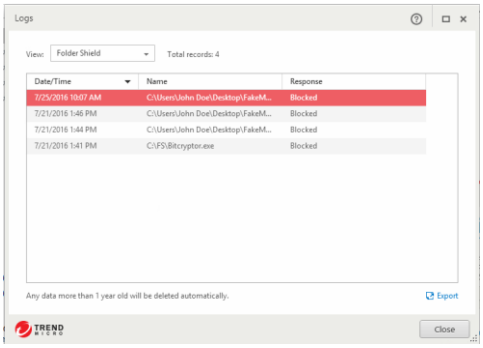



**Figure 222. Folder Shield Logs**

11. Click **Export** if you wish to export the table for future reference or for troubleshooting with a Trend Micro Support expert.
12. Click **Close** to close the table, then **OK** to close the warning popup.

# Family: Upgrade Now

Keep your family safe online by upgrading to **Trend Micro Maximum Security** for **Parental Controls.**

**To get Parental Controls:**

1. Open the Trend Micro Security Console.

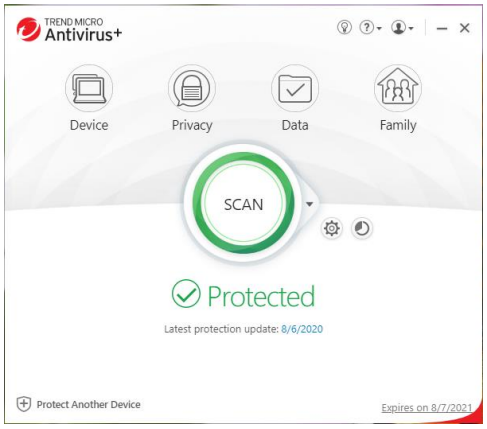



**Figure 223. Console > Family**

2. Click the **Family** icon. The **Family** screen appears.

**Figure 224. Family**

1. Click **Upgrade Now** and follow the online instructions to upgrade to **Trend Micro Maximum Security** to enable **Parental Controls**.
2. By upgrading to **Maximum Security**, you can
   - Restrict or filter your children's access to websites and programs
   - Help manage online reputation of your children
   - Block inappropriate images in web search results.

# Chapter 5: Trend Micro Internet Security

This chapter provides detailed instructions for configuring and using Trend Micro Internet Security. All features described in this chapter are also included in Trend Micro Maximum Security.

## Protection Overview

**Trend Micro Internet Security** provides everything included in **Trend Antivirus+ Security**, but adds some significant protections and tools, outlined below. To enable all functions, you need a paid version of Internet Security.

**Figure 225. Trend Micro Internet Security Console**

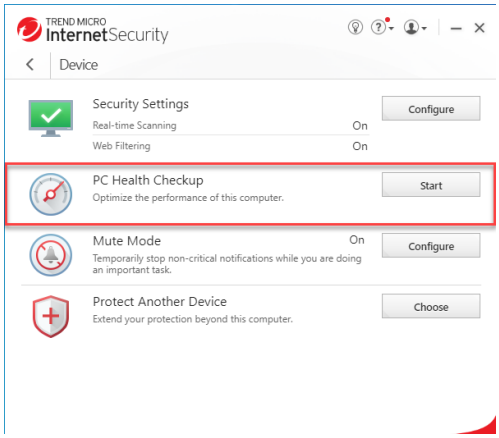



**Figure 226. Device > PC Health Checkup**

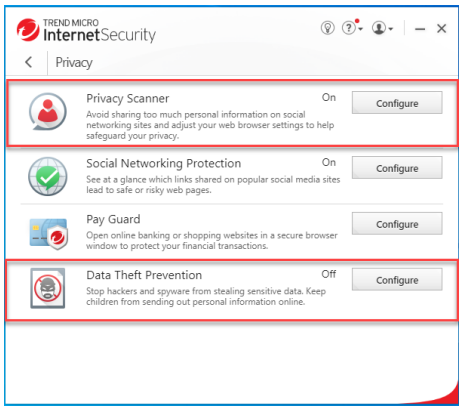



**Figure 227. Privacy > Privacy Scanner | Data Theft Prevention**

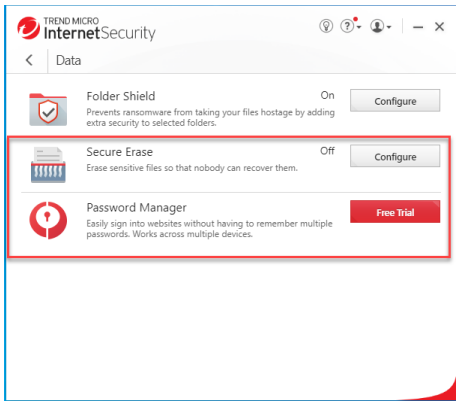



**Figure 228. Data > Secure Erase | Password Manager Free Trial**

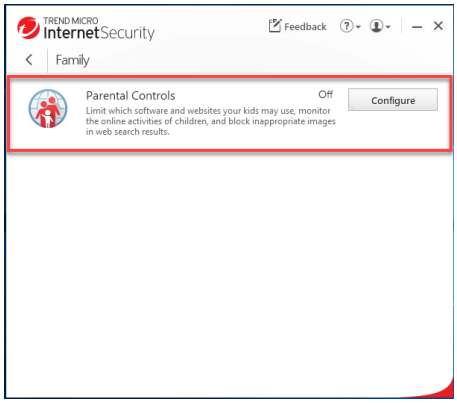



**Figure 229. Family > Parental Controls**

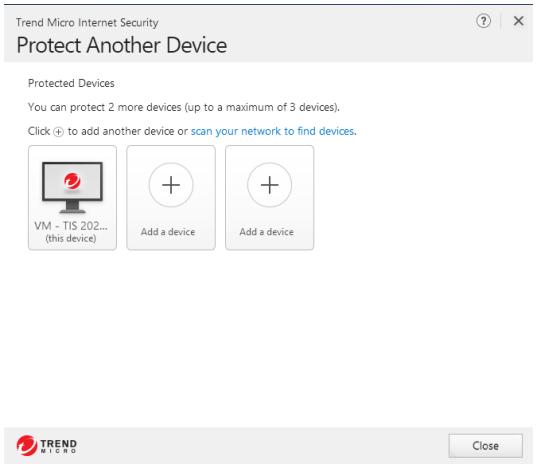



**Figure 230. 3-Device Option – Windows and Mac**

**Note:** **Trend Micro Internet Security has additional features beyond Trend Micro Security Antivirus +. These include**

**Device: Smart Scheduled Scans, PC Health Checkup**

**Privacy: Privacy Scanner, Data Theft Prevention**

**Data: Secure Erase and Free Trial Offer for Password Manager**

**Family: Parental Controls**

**Additional Seats: 3-Device Option – Windows and Mac: Protect 2 more devices or scan your network to find devices.**

## ADDITIONAL TOOLS FOR TREND MICRO SECURITY INTERNET SECURITY PAID VERSION

### Smart Schedule Scans

Trend Micro Internet Security provides a new way to conduct scheduled scans with its Smart Schedule. Based upon recent computer usage, the most suitable scan will start automatically at an appropriate time.

### PC Health Checkup

Trend Micro Internet Security adds the **PC Health Checkup**, which can improve PC performance by cleaning up temporary files, registries, and the Start-up Manager. It also checks for potentially incompatible programs (PIPs). Reports provide information on how your computer has been optimized.

### Privacy Scanner

Trend Micro Internet Security adds **Privacy Scanner** for Facebook, Twitter, and LinkedIn, and the Internet Explorer, Google Chrome, and Mozilla Firefox browsers. The Privacy Scanner scans your privacy settings, alerts you to settings that expose you to potential identity theft, and lets you automatically change them.

### Data Theft Prevention

With its **Data Theft Prevention** feature, Trend Micro Internet Security allows you to prevent data leakage (from email and instant messaging tools) or data theft (from tools such as keyloggers).

### Secure Erase

Trend Micro Internet Security also adds **Secure Erase**, which shreds computer files that have sensitive information, making it impossible for an unauthorized person to recover them.

### Parental Controls

Trend Micro Internet Security allows parents to restrict access to websites by users, rule sets, and categories. **Parental Controls** also gives parents the ability to limit the amount of time their child is allowed to use the Internet. Trend Micro Security's Parental Controls tap into Windows User Accounts, assigning each rule set to a specific user.

### Password Manager

Trend Micro Internet Security provides easy download access to a Free Trial 5-account version of Trend Micro Password Manager, which helps you to manage all your online credentials. Trend Micro Security users can buy the full version for unlimited password management.

### Protect Another Device: Windows and Mac

Trend Micro Internet Security's allows you to protect up to three Windows and Mac devices. For example, when you click the Mac icon in **Protect Another Device**, you can email an install link, copy a link, or directly download Trend Micro Antivirus for Mac. You can also scan your network to find other devices to protect.

# Device: Security Settings: Security & Tuneup Controls > Smart Scheduled Scan

Trend Micro Internet Security provides a new way to conduct scheduled scans with its Smart Schedule. Based upon recent computer usage, the most suitable scan will start automatically at an appropriate time.

**To view Smart Schedule scan:**

**Figure 231. Trend Micro Internet Security Console**

1. In the **Trend Micro Internet Security Console**, click **Device.** The **Device** window appears.

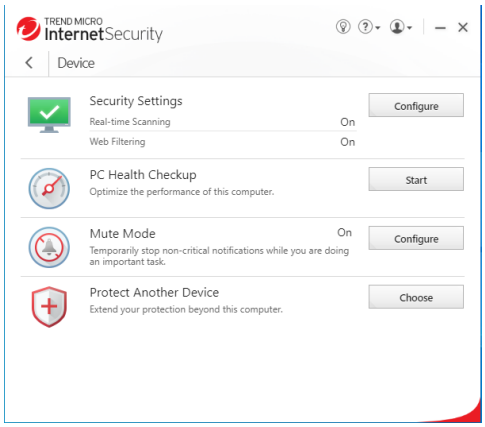



**Figure 232. Device**

2. Click **Configure** in the **Security Settings** panel. The **Security & Tuneup Controls** window appears, with **Scan Preferences** selected by default.

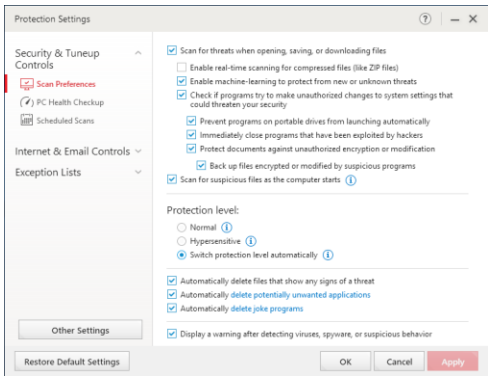



**Figure 233. Security & TuneUp Controls > Scan Preferences**

3. Click **Scheduled Scans.** The **Scheduled Scans** screen appears.

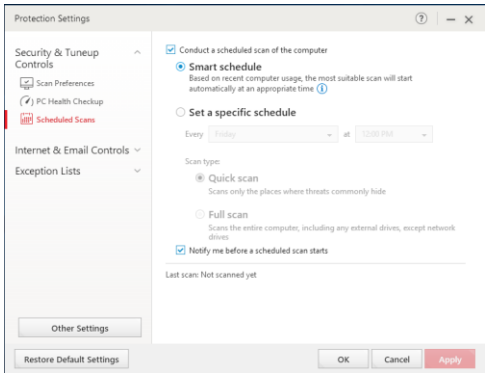



**Figure 234. Scheduled Scans > Smart Schedule**

4. Observe that **Smart Schedule** is chosen by default. If you leave this setting as is, **Trend Micro Internet Security** will itself decide, based on your recent computer usage, when the most suitable scan (Quick or Full) should be conducted.

5. Alternately, you may **Set a specific schedule**, along with **Scan type** (Quick or Full), as described in the previous chapter.

6. The option **Notify me before a scheduled scan starts** is turned on by default. Uncheck the checkbox if you do not wish to be notified.

# Device: PC Health Checkup | Security Settings

Trend Micro Internet, Maximum, and Premium Security provide a **PC Health Checkup** that can help you recover disk space, make Microsoft Windows start faster, clean up your instant messaging history, and optimize your computer's performance. You can also plan scheduled tune-ups that can automatically keep everything running smoothly.

**Note:** **PC Health Checkups are automatically performed whenever you do a Quick or Full Scan, but you can also conduct a PC Health Checkup on its own.**

## Perform a PC Health Checkup

**To perform a PC Health Checkup:**

1. Click **Device > PC Health Checkup > Start** in the **Console**.

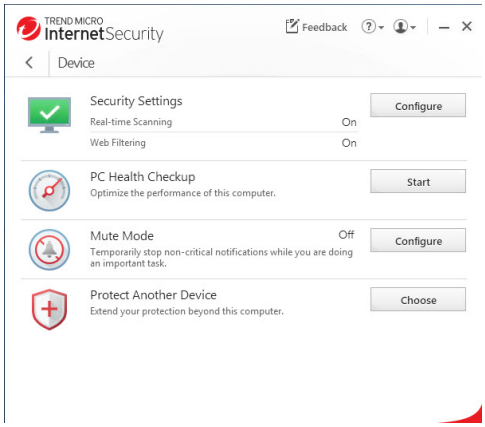



**Figure 235. Device > PC Health Checkup**

2. A **PC Health Checkup** scan begins immediately, showing the progress of the optimization.

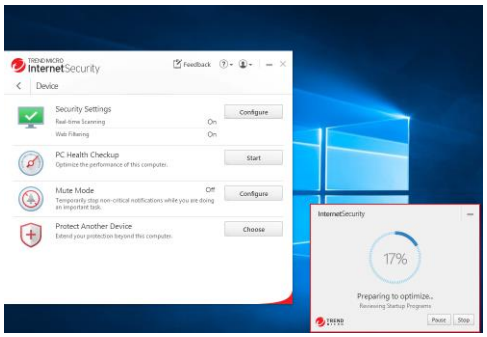



**Figure 236. Device > PC Health Checkup > Start**

3. When the scan completes, a **Results** screen appears, providing an indicator of your Optimization Level—in this case, **Very Good**, suggesting possible improvements.

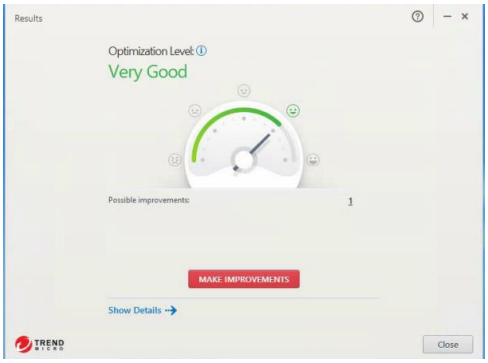



**Figure 237. PC Health Checkup Results**

4. Click **Make Improvements** to make the improvements. **PC Health Checkup** makes the improvements to your system.

5. You can also click **Show Details** to obtain more details about the suggested improvements. The **Details** screen appears.

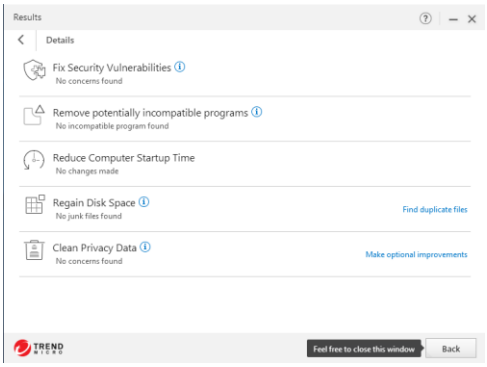



**Figure 238. PC Health Checkup Details**

6. Details include the following:

   - Fix Security Vulnerabilities
   - Remove potentially incompatible programs
   - Reduce Computer Startup Time
   - Regain Disk Space
   - Clean Privacy Data

7. Again, click **Make Improvements** to make the improvements; the results will be displayed.

8. Click **Back** to return to the **Optimization Level** window. The level will be adjusted to show your improvements.

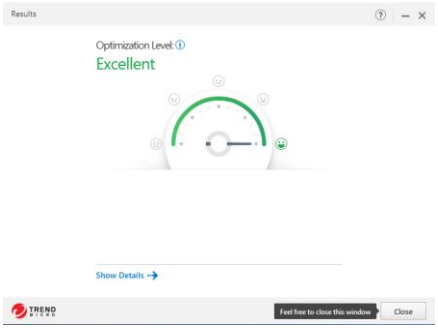



**Figure 239. Optimization Level: Excellent**

9. Click **Close** to close the **Optimization Level** window. This returns you to the **Device Settings** window.

## Configure PC Health Checkup

**To configure PC Health Checkup:**

1. Back in the main **Console** screen, click **Device > Security Settings > Configure.** The **Protection Settings** screen appears, with **Security & Tuneup Controls > Scan Preferences** shown by default.

2. Click **PC Health Checkup** to configure its settings.

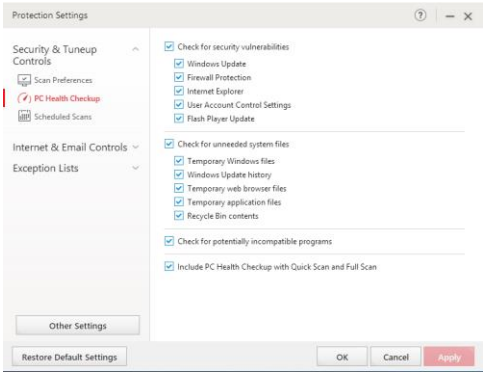



**Figure 240. PC Health Checkup Settings**

3. You can define how **PC Health Checkup** works by checking/unchecking a **Security Vulnerability** or **Unneeded System Files** item. All items are checked by default.

   **Check for security vulnerabilities**

   - Windows Update
   - Firewall Protection
   - Internet Explorer
   - User Account Control Settings
   - Flash Player Update

**Check for unneeded system files**

- Temporary Windows Files
- Windows Update history
- Temporary web browser files
- Temporary application files
- Recycle Bin contents

**Check for potentially incompatible programs.** Uncheck to disable this in your PC Health Checkup.

**Include PC Health Checkup with Quick Scan and Full Scan.** Uncheck this to disable PC Health Checkup with Quick and Full scans.

4. Click **Apply** to apply any changes.

## Security Report: PC Health Checkup

Once you have conducted one or more PC Health Checkups, you can view a **PC Health Checkup Security Report.**

**To view a PC Health Checkup Security Report:**

1. Open the Trend Micro Security Console.

**Figure 241. Security Report Tool**

2. Click the **Security Report** tool. The **Security Report** appears, with **Security Threats** selected by default.

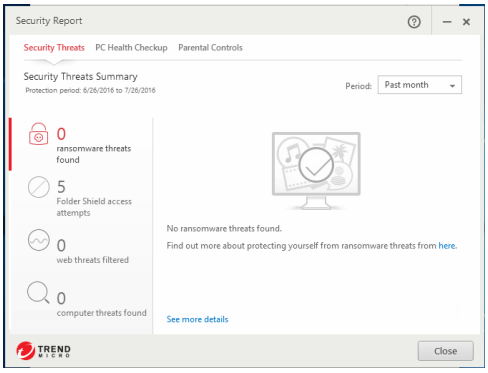



**Figure 242. Security Threats**

3. Click the **PC Health Checkup** menu item to display a **Report**.

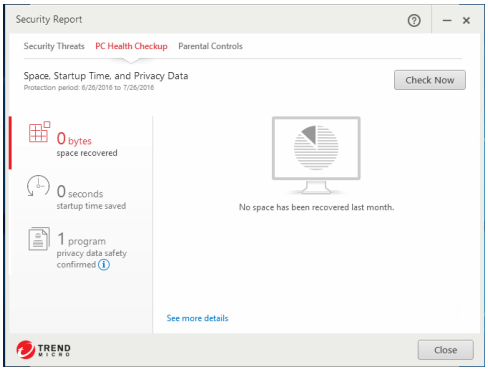



**Figure 243. PC Health Checkup Report**

4. Click **See more details** to obtain tabular data on Security and PC Health Checkup results.

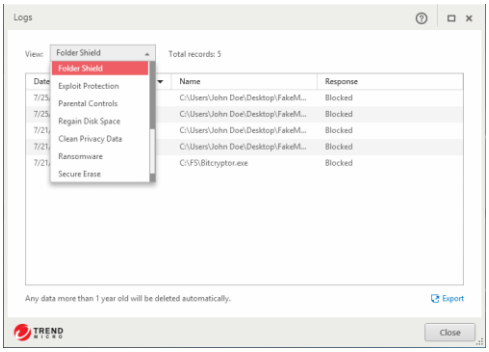



**Figure 244. PC Health Checkup Logs**

5. Use the **View** drop-down menu to view different logs, including **Regain Disk Space** and **Clean Privacy Data.**

6. Click **Export** to export the log in .CSV or .TXT format.

7. Click **Parental Controls** to see the report on **Parental Controls.** (Not yet set up. Click **Set UP** to set up. Go to Family: Parental Controls for the setup process.)

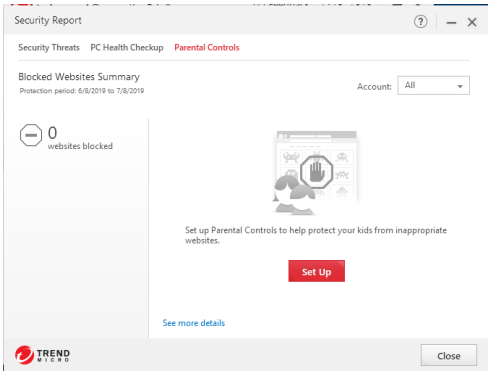



**Figure 245. Security Report for Parental Controls**

8. Monthly **Security Reports** are automatically generated by Trend Micro Security and emailed to you at the email address you used to create your account. Your monthly report includes

   - A list of Computers Protected in your account
   - A Threat Summary, including the various types of threats detected
   - A PC Health Checkup, including amount of space recovered and seconds saved at startup
   - Parental Controls, including violations of web and usage rules
   - An invitation and button to protect other devices, the number of which depends upon your active Trend Micro licenses.

# Device: Protect Another Device

Trend Micro Internet Security provides a subscription for three Windows or Mac devices, including Windows devices in S Mode. Periodically, a popup will appear reminding you that you can protect more devices, as well as click **Scan Network** to apply your subscription to the devices the scan finds.

**Figure 246. Scan Network**

Go to **Protect Another Device: PCs, Macs, Android and iOS Mobile Devices** for more details.

# Privacy: Privacy Scanner: Social Network Privacy & Web Browser Privacy

The Trend Micro Security **Privacy Scanner** works with Facebook, Twitter, and LinkedIn and supported PC browsers (Chrome, Firefox, Edge, and Internet Explorer). It's turned on by default in Trend Micro Internet and Maximum Security. The default setting also turns on the Trend Micro Toolbar, which can be used to launch the Privacy Scanner.

**NOTE: Make sure the Trend Micro Toolbar is already enabled in your browser before you try to use the Privacy Scanner. See Enable Trend Micro Toolbar for details.**

**To use the Privacy Scanner:**

1. Double-click the Trend Micro Security shortcut on the desktop to open the **Trend Micro Security Console**. The **Trend Micro Security Console** appears.

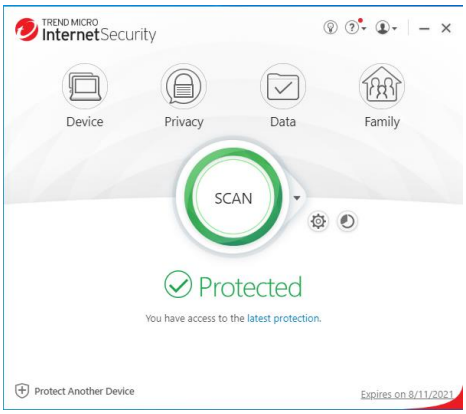



**Figure 247. Trend Micro Security Console > Privacy**

**Do one of two things:**

2. In the main **Console** window, click the **Privacy** icon. The **Privacy** window appears.

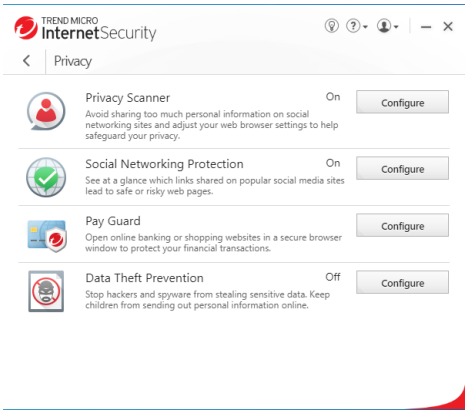



**Figure 248. Privacy > Facebook Privacy Scanner**

3. Click **Configure** in the **Privacy Scanner** panel. The **Privacy Scanner** window appears.

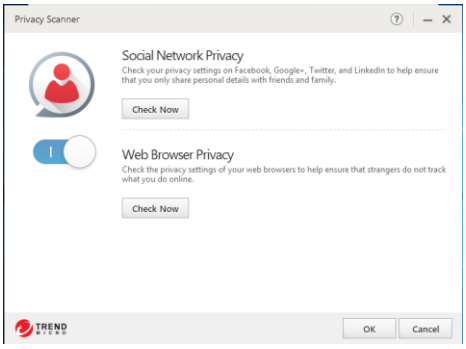



**Figure 249. Privacy Scanner window**

4. Ensure the slider is **On** and click **Check Now** in the **Social Network Privacy** panel.

**OR:**

5. Open your browser and select the **Trend Micro Toolbar > Check your online privacy**.

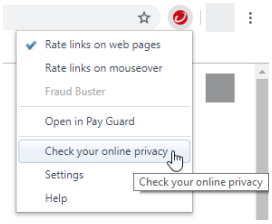



**Figure 250. Check your online privacy**

6. Both actions take you via your browser to the **Trend Micro Privacy Scanner** webpage, with the **Facebook** sign-in panel shown by default.

## Facebook Privacy Settings

**To check your Facebook Privacy Settings:**

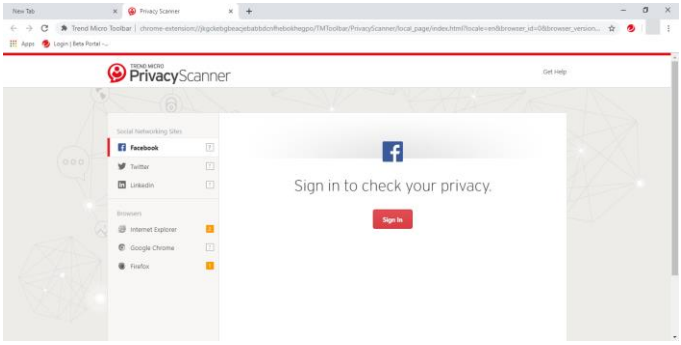



**Figure 251. Trend Micro Privacy Scanner | Facebook**

1. In the **Privacy Scanner** page, click **Sign In**. Trend Micro Security automatically takes you to the Facebook login website.

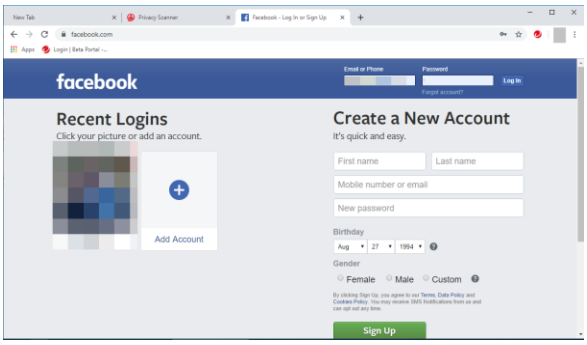



**Figure 252. Facebook Login Webpage**

2. Sign in to your Facebook account. The **Facebook News Feed** page displays, showing Trend Micro Security's **Privacy Scanner for Facebook**.

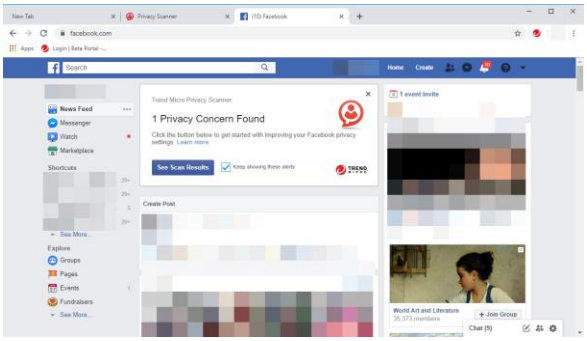



**Figure 253. Facebook > Check My Privacy**

3. Click **See Scan Results**. Facebook returns the results, indicating when you have privacy concerns.

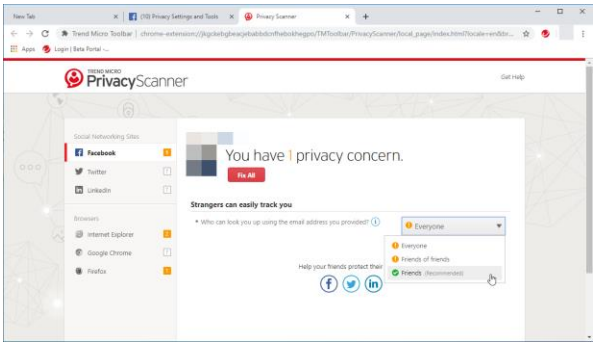



**Figure 254. Facebook Privacy Concerns**

4. If you have concerns, click **Fix All** to fix all the concerns at once using the Trend Micro Security recommended privacy settings, or select the drop-down settings menu to fix them manually. In this example, we'll choose **Fix All**. The **Fix** popup appears.

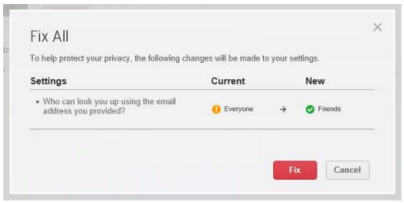



**Figure 255. Fix All | Editor**

5. Click **Fix** for the settings with Privacy Concerns. Trend Micro Security changes your settings and returns the result. In this case, since you accepted the default recommendations, it returns "Nice work! You don't have any privacy concerns, but your friends might need some help..."

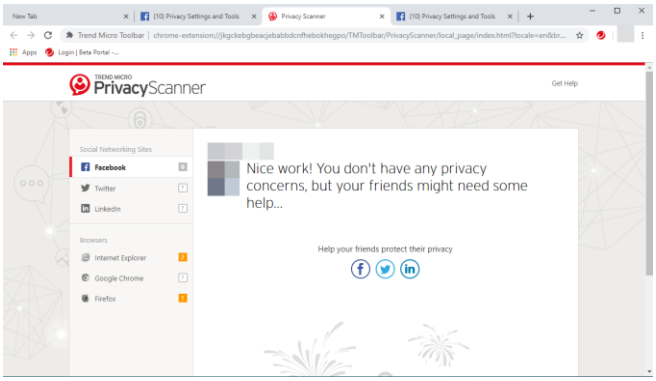



**Figure 256. Nice work!**

6. Click the **Facebook** icon to share a link Trend Micro Security and the Privacy Scanner to your friends on **Facebook**. The **Share Link** screen appears, allow you to share the post on Facebook.

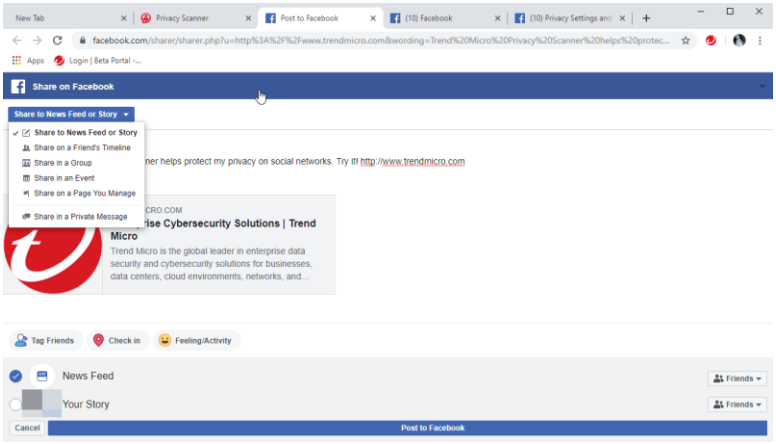



**Figure 257. Share to Facebook**

**Upper-left popup:**

- Share to News Feed or Story
- Share on a Friend's Timeline
- Share in a Group
- Share in an Event
- Send on a Page You Manage
- Share in a Private Message

7. Choose an option, or simply click **Post to Facebook.** The link is posted according to your choice.

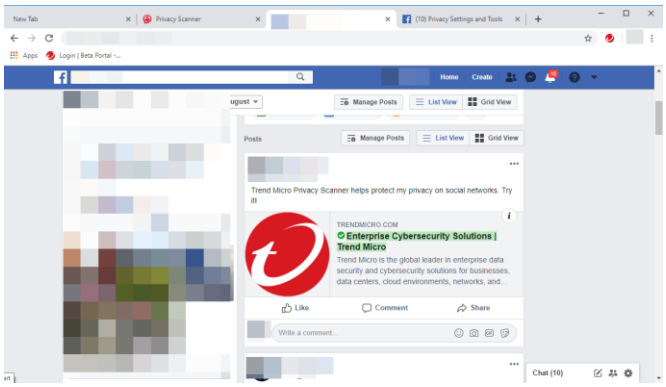



**Figure 258. Trend Micro - Shared Link**

## Facebook App Privacy Settings

Note that the Privacy Scanner also scans Facebook Apps for their privacy settings. When you use a social networking app on your Facebook page, such as a game, your privacy settings determine who can see your posts.

**To check the privacy settings of your app or game:**

1. Use **Privacy Scanner** to perform a Privacy Scan of Facebook, as explained in the previous section. Trend Micro Security provides the result.

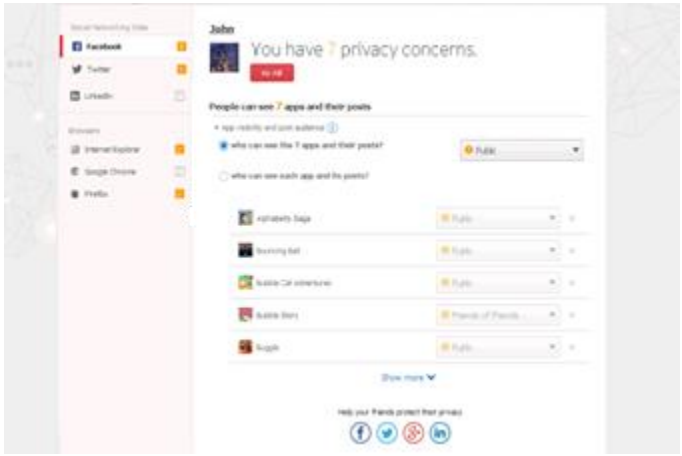



**Figure 259. Apps (Games) With Privacy Concerns**

2. Select **Fix All**, then **Fix** in the popup, to fix all your app privacy settings at once, or select "Who can see each app and its posts?", then fix each app setting in turn. Facebook tells you "Nice work! You don't have any privacy concerns, but your friends might need some help."

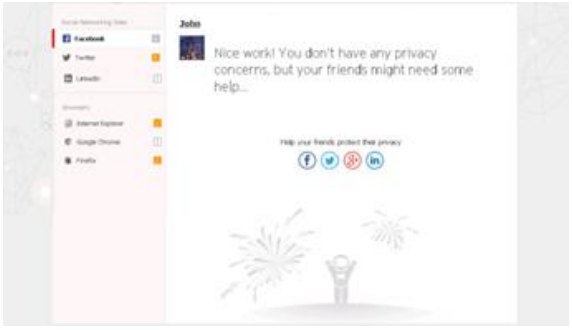



**Figure 260. Nice Work! You don't have any privacy concerns.**

## Twitter Privacy Settings

**To check your Twitter Privacy Settings:**

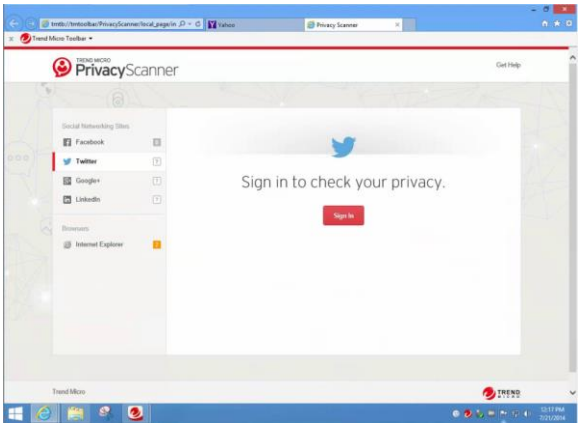



**Figure 261. Privacy Scanner | Twitter**

1. Click the **Twitter** tab in **Trend Micro Privacy Scanner**. The **Twitter Log In** page opens in your browser. Click the tab to access it.

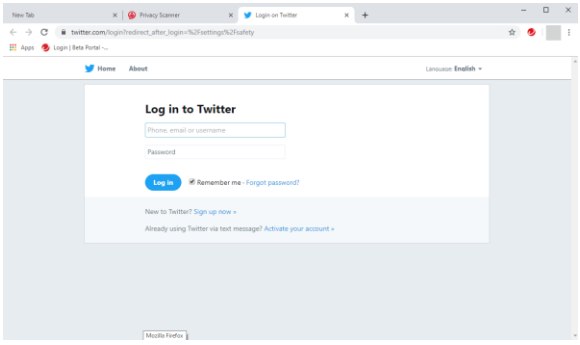



**Figure 262. Log in to Twitter**

2. Sign in to your Twitter account. Your **Twitter Settings** page appears.

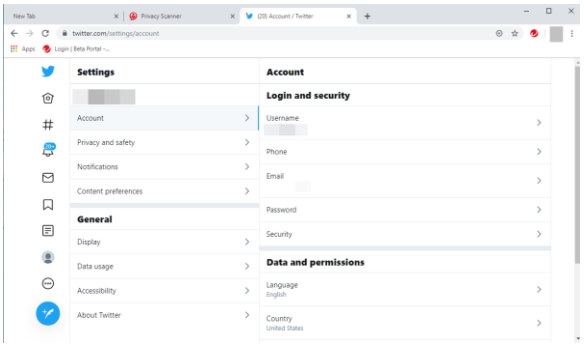



**Figure 263. Twitter > Settings**

3. Tap the **Privacy Scanner** tab. The Trend Micro Privacy Scanner returns the result.

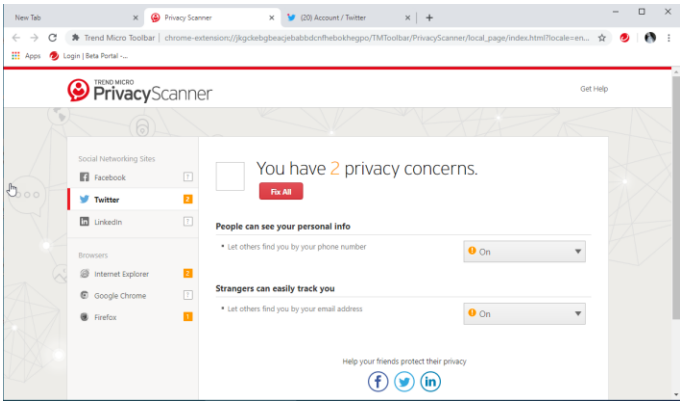



**Figure 264. Twitter Privacy Concerns**

4. As you did for Facebook, click **Fix All** or use the editor to edit specific settings. The editor appears.

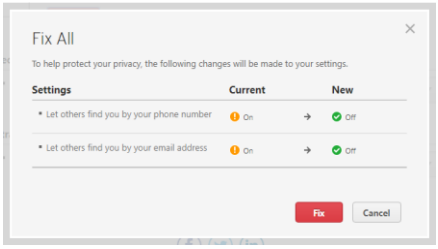



**Figure 265. Fix All | Settings**

5. Click **Fix** to fix your settings. Twitter requires that you enter your password to make changes to your account.

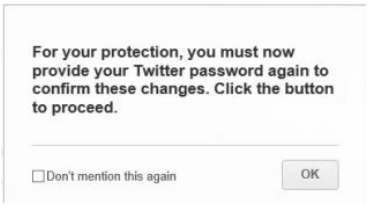



**Figure 266. Twitter Password Request**

6. Click **OK** to proceed. The **Save account changes** dialog appears.

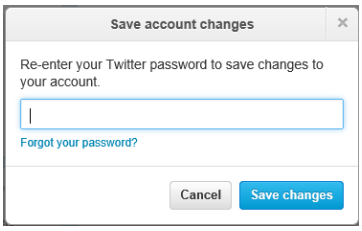



**Figure 267. Save Account Settings**

7. Re-enter your Twitter password and click **Save Changes.** Twitter saves the changes.
8. When the **OK** dialog reappears, click **OK** again to ensure you have no remaining privacy concerns. The **Privacy Scanner** returns the result: “Nice work! You don’t have any privacy concerns, but your friends might need some help…”

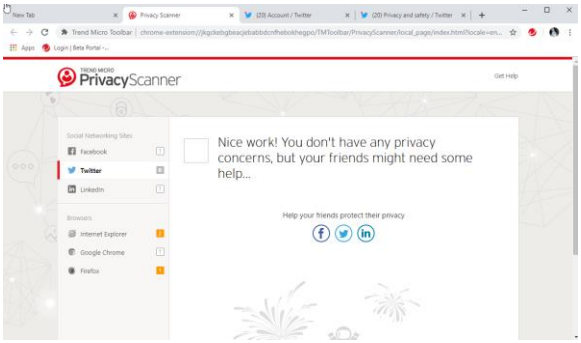



**Figure 268. Privacy Scanner: No Privacy Concerns**

9. As you did for Facebook, you can click the Twitter icon to post a link to help your friends protect their privacy.

## LinkedIn Privacy Settings

**To check your LinkedIn Privacy Settings:**

1. Click **LinkedIn** in the **Privacy Scanner** list to begin a privacy scan of LinkedIn. The **LinkedIn Sign In** page appears.

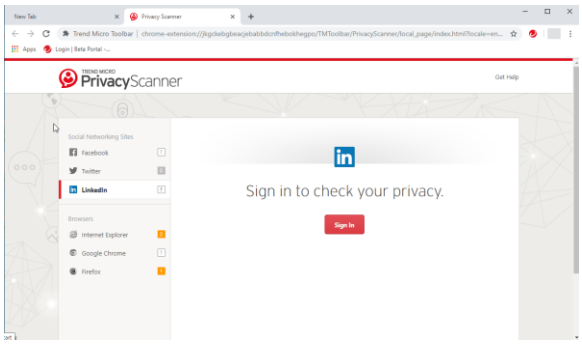



**Figure 269. LinkedIn Sign In**

2. Click **Sign in** to sign in to Linked In.

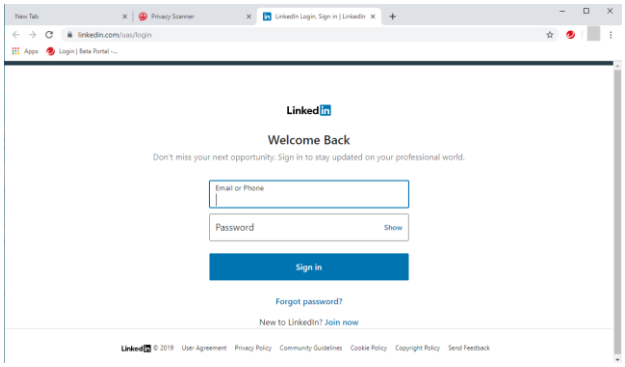



**Figure 270. Sign In to LinkedIn**

3. Enter your LinkedIn email address and password and click **Sign In.** Linked In opens and a **Privacy Scanner** panel appears in your LinkedIn page.

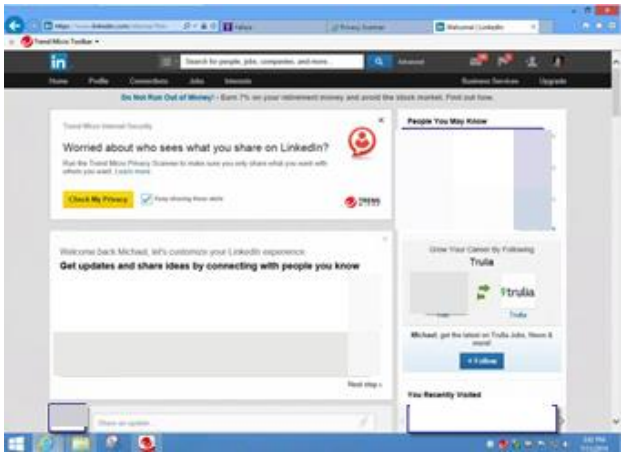



**Figure 271. LinkedIn > Check My Privacy**

4. Click **Check My Privacy** to begin a privacy scan of LinkedIn. **Privacy Scanner** scans your privacy settings and returns the result.

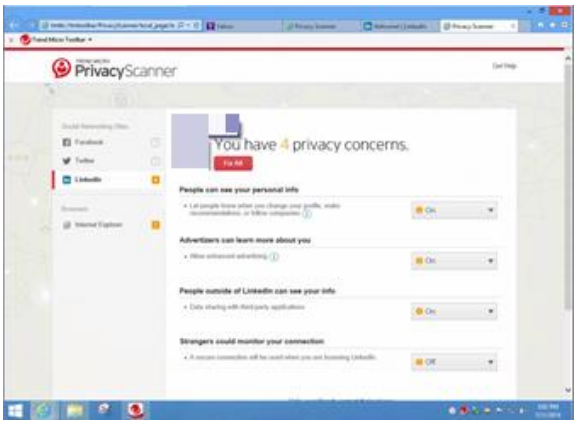



**Figure 272. LinkedIn > 4 Privacy Concerns**

5. As before click **Fix All** or use the editor to edit each manually. For the **Fix All** option, the **Fix All** dialog appears.

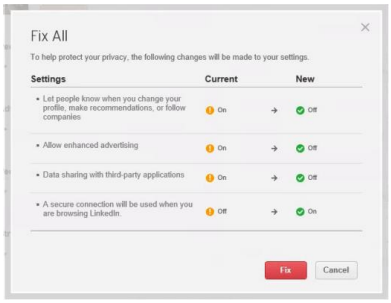



**Figure 273. Fix All**

6. Click **Fix** to fix all the privacy concerns.

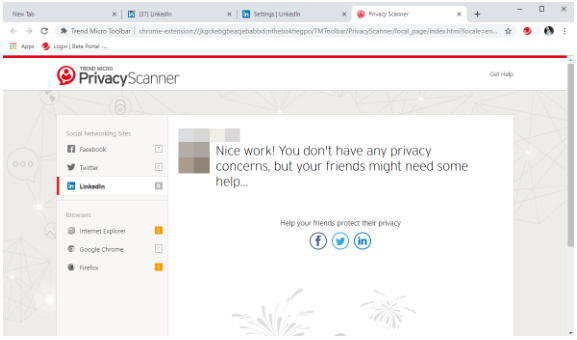



**Figure 274. Nice Work! No Privacy Concerns**

7. Privacy Scanner returns the result and the familiar “Nice Work!” page appears, where you can again help your friends protect their privacy by clicking the **LinkedIn** icon to post a link.

8. Trend Micro Security provides ongoing protection for Facebook, Twitter, Google+, and LinkedIn. At any time, particularly when the social networking site changes any privacy

policies, you can run another **Privacy Scan** on your social networking pages to check your privacy settings.

## Web Browser Privacy Settings

Trend Micro Security **Privacy Scanner** scans your Web browsers, including **Internet Explorer, Google Chrome,** and **Mozilla Firefox**, to ensure maximum privacy as you're browsing the internet.

1. To initiate a browser scan, simply open your preferred Web browser; for example, Internet Explorer.

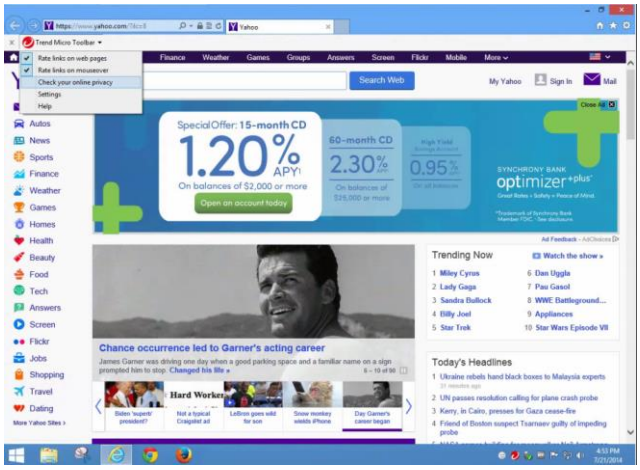



**Figure 275. Internet Explorer > Check your online privacy**

2. In the **Trend Micro Toolbar,** select **Check your online privacy**. The **Trend Micro Privacy Scanner** portal appears, with **Facebook** selected by default.

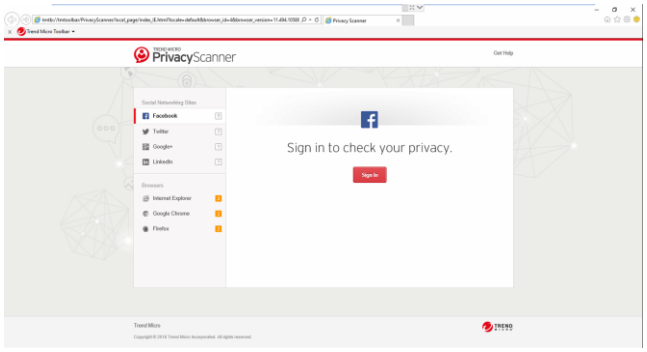



**Figure 276. Trend Micro Privacy Scanner Portal**

3. Click the installed Web browser you wish to check in the **Browsers** section; for example, **Internet Explorer.** The **Privacy Scanner** shows when you have privacy concerns.

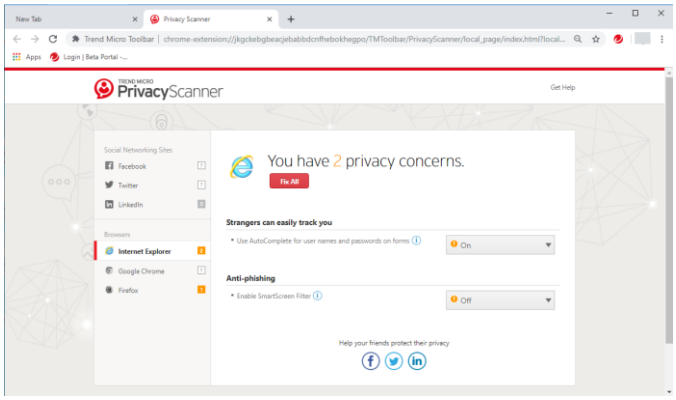



**Figure 277. Privacy Scanner > Internet Explorer**

4. Click **Fix All** to fix all the privacy concerns, or manually edit them. When you click **Fix All**, the **Fix All** dialog appears.

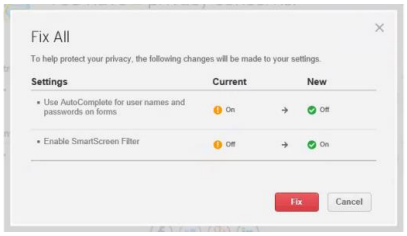



**Figure 278. Fix All**

5. Click **Fix** to fix the privacy concerns. **Privacy Scanner** resets the privacy settings in your browser and provides a Restart dialog to complete the process.

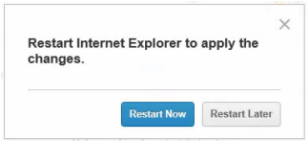



**Figure 279. Restart Now**

6. Click **Restart Now** to apply the changes. The browser restarts with the changed privacy settings, saying “Nice Work! You don’t have any privacy concerns, but your friends might need some help…”

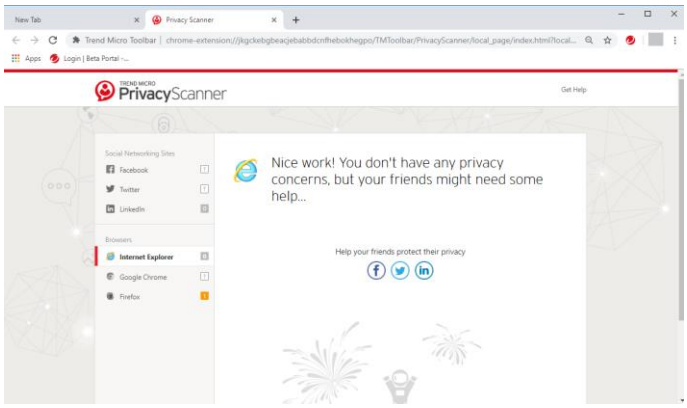



**Figure 280. Nice Work!**

7. Repeat this process for each of your installed browsers.
8. Note that you can reset your privacy settings for any supported browser (**Internet Explorer, Chrome,** or **Firefox**) from *within that browser* for any of the *other* supported browsers installed on your computer.

# Privacy: Data Theft Prevention

**Data Theft Prevention** prevents hackers and spyware from stealing sensitive data like credit card numbers, passwords, and email addresses. It can also stop children from accidentally sending out personal information through Outlook email, via instant messaging, or to untrustworthy websites.

To activate **Data Theft Prevention** in Trend Micro Security Internet Security (or Maximum and Premium Security) you must first create an email address and password. See the previous section for **Trend Micro Security Antivirus+** to obtain instructions on doing this.

**To activate Data Theft Prevention:**

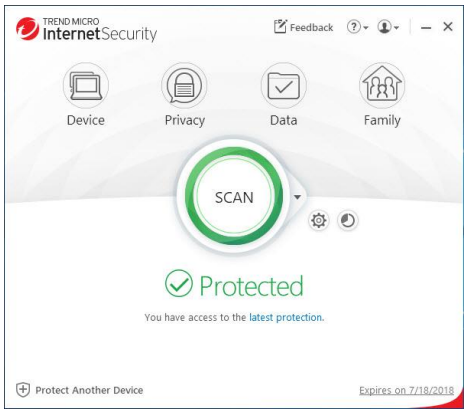



**Figure 281. Trend Micro Internet Security Console**

1. Click **Privacy** icon in the Console. The **Privacy** screen appears, showing the tools available.

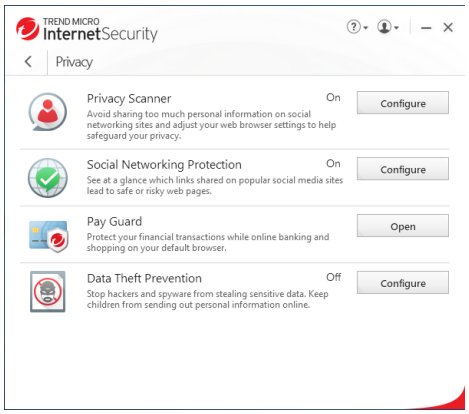



**Figure 282. Privacy Options**

2. Click **Configure** in the **Data Theft Prevention** panel. Trend Micro Internet Security provides you with an introduction to **Data Theft Prevention.**

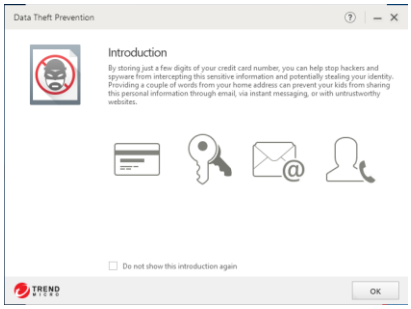



**Figure 283. Data Theft Prevention Introduction**

3. Click **OK** to close the introduction. The **Password** screen appears. A password is required to use **Data Theft Prevention** or **Parental Controls** in Trend Micro Security.

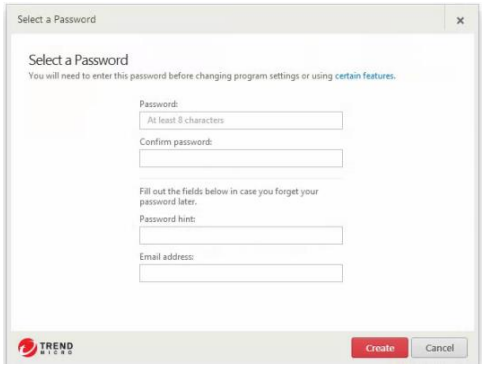



**Figure 284. Select a Password**

4. Enter a password and confirm it. Fill out the **Password hint** and **Email address**, in case you forget your password later. This will enable Trend Micro to send you a new password. Then click **Create**. The **Data Theft Prevention** settings screen appears, with the toggle set to **Off** by default.

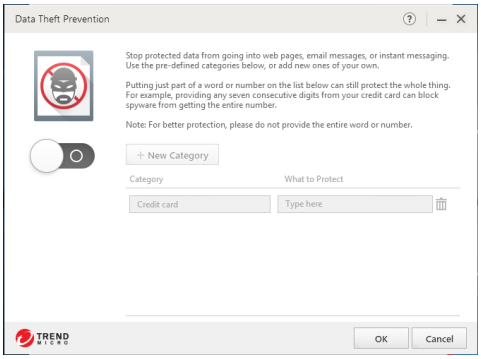



**Figure 285. Data Theft Prevention**

5. Click the slider to **On** to enable **Data Theft Protection.**
6. Trend Micro Security Internet Security provides you with some suggested categories such as **Phone number** and **Credit card.** You can edit any existing category name by typing over it. For better protection, don't provide the entire word or number.
7. In the **What to Protect** column, type the actual data you wish to protect; for example, in the phone number field you might type 899-999
8. After you save it, Trend Micro Security hides it from view by using asterisks. Simply click in the field to make it visible.
9. Click **+New Category** to add a new category.
10. Click the trashcan in the right-hand column of **What to Protect** to delete any category.
11. Click **Ok** to save your changes.

**DTP Limitations**

- Data Theft Prevention won't protect the receiving data via POP3 traffic.
- Data Theft Prevention monitors HTTP traffic (ports 80, 81, 8080, and any proxy server port you configure in your Microsoft® Internet Explorer® settings), but not HTTPS traffic (i.e., encrypted information cannot be filtered, such as webmail).
- Data Theft Prevention uses SMTP on TCP port 25/587 and is blocked as spec. TLS and SSL encryption authentication don't block as spec. Most free webmail programs provide TLS and SSL encryption authentication such as Hotmail, Gmail, and Yahoo! Mail.
- Data Theft Prevention doesn't monitor "IMAP" traffic as spec. An IMAP server is generally used with programs such as Microsoft Exchange Server, Hotmail, Gmail, AOL Mail.
- Data Theft Prevention can protect a maximum of 20 entries that have different data and categories.

# Data: Secure Erase

Deleting a file just removes the directory information used to find it, not the actual data. The **Secure Erase** function provided in Trend Micro Internet Security (and also in Maximum and Premium Security) overwrites the unwanted file with data, so no one can retrieve the contents; while **Permanent Erase** overwrites the unwanted files making seven passes (overwriting the files 21 times, meeting US Government Security Standards).

**To enable Secure Erase / Permanent Erase:**

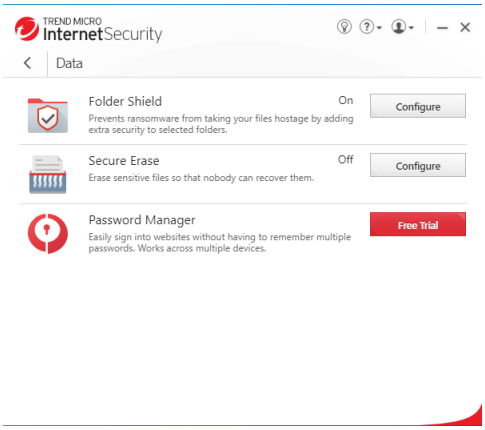



**Figure 286. Secure Erase**

1. In the main **Console**, click **Data**, then **Configure** for **Secure Erase.** The **Secure Erase Introduction** window appears.

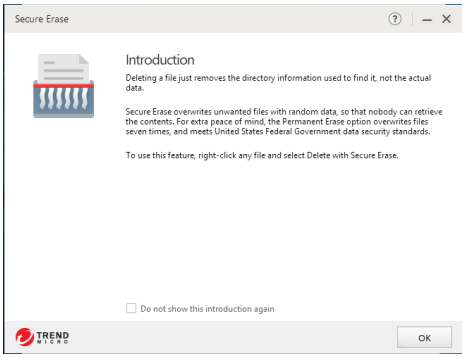



**Figure 287. Secure Erase Introduction**

2. Click **OK** to close the **Introduction** window. The **Type of Erase** window appears, with **Quick Erase** selected by default.

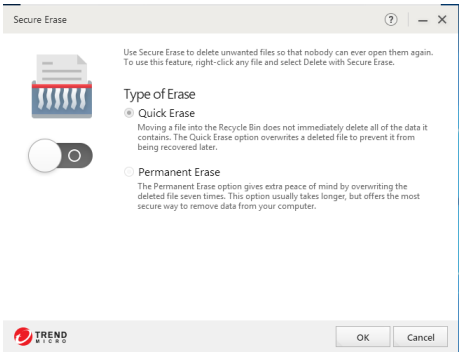



**Figure 288. Type of Erase**

3. Move the toggle to **On** to enable the function.
4. Keep **Quick Erase** or select the **Permanent Erase** button.
5. Click **OK** to save your changes.

**To Secure/Permanent Erase a file:**

1. Right-click a folder or file to perform a **Quick/Permanent Erase**. A file processing popup appears.

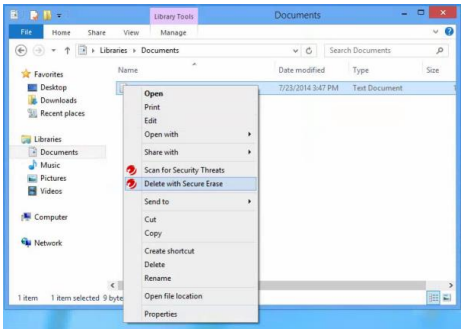



**Figure 289. Right-click File for Secure Erase**

2. Select **Delete with Secure Erase / Permanent Erase.**
3. The folder or file is securely deleted.

# Data: Password Manager - Free Trial

**Trend Micro™ Password Manager** lets you easily sign into websites without having to remember multiple passwords. A **Free Trial for Password Manager**—which allows you to save up to 5 passwords—is available for download from the Trend Micro Internet Security Console.

**Note:** **A full, unlimited version of Trend Micro Password Manager is automatically installed with Trend Micro Maximum and Premium Security. See the following chapter for details:** **Data: Password Manager - Full Version**

Features include:

- **URL and Password Management -** Automatically capture your websites and password login credentials in a complete secure environment
- **Multi-user Access** – Multiple users can use Password Manager on the same computer.
- **Web Console Management** – Password Manager lets you use a Web Management Console to manage your passwords, notes, and other credentials. The Web Management Console also provides a password strength indicator, to increase the security of your accounts.
- **Cloud Storage and Synchronization -** Credentials are available across all devices where Password Management is installed
- **Password Generator -** Automatically generate strong passwords with custom criteria for increased login security
- **Secure Notes Management -** Store and manage Secure Notes regarding your accounts, logins, and procedures.
- **Password and Data Encryption –** All passwords entered in supported browsers are encrypted. AES 256-bit Encryption ensures the highest security for your data.

- **Secure Browser -** Use the Secure Browser on the PC and Mac to ensure security and privacy for online financial transactions.
- **Profile for Auto-Form Filling -** Create a Profile to enable auto-form filling when filling out online forms.
- **Mobile Support -** iOS and Android smartphones and tablet devices are fully supported.

**To Download and Install Password Manager:**

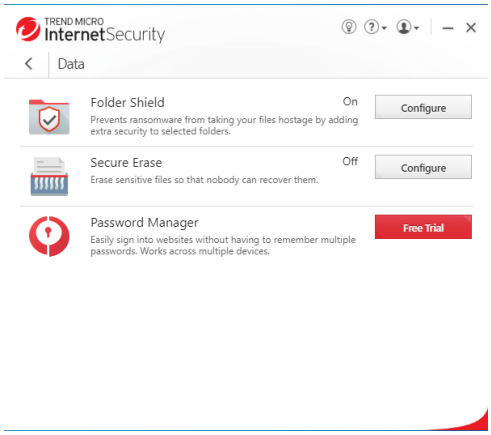



**Figure 290. Data > Password Manager Free Trial**

4. In the **Main Console**, click **Data**, then **Free Trial** for **Password Manager**. Your default browser launches the **Password Manager Software** page.

**Figure 291. Password Manager Software**

5. Click **Get it for free.** The **Password Manager Download** page appears.

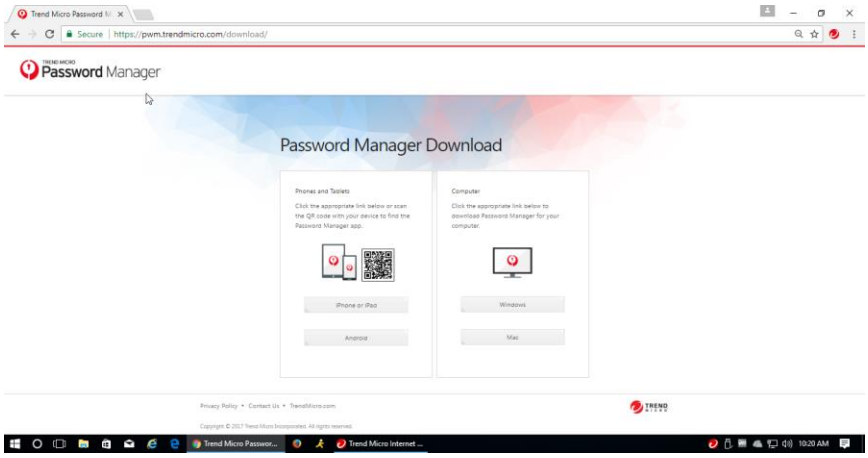



**Figure 292. Password Manager Download**

6. Choose the platform you're on and click the download button. **Password Manager** downloads and presents you with a **Run / Save** dialog in Internet Explorer. In Chrome or Firefox you're simply presented with the exe file.

**Figure 293. Internet Explorer – Run**

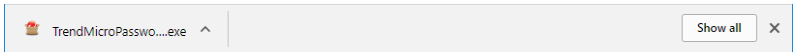



**Figure 294. Chrome - EXE**

7. Click **Run** or double-click the **EXE** file to begin the installation. The **Password Manager Installer** begins the install process, and the **User Account Control** dialog appears.

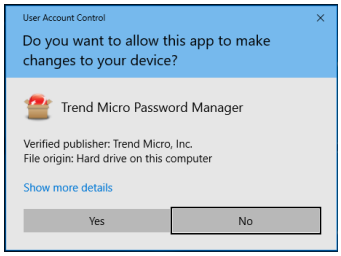



**Figure 295. User Account Control**

8. Click **Yes** to continue. Password Manager **Downloader** downloads the file.

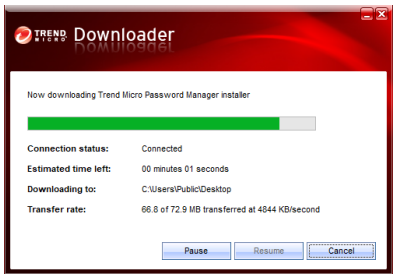



**Figure 296. Password Manager Downloader**

9. The installer then presents you with the **License Agreement**.

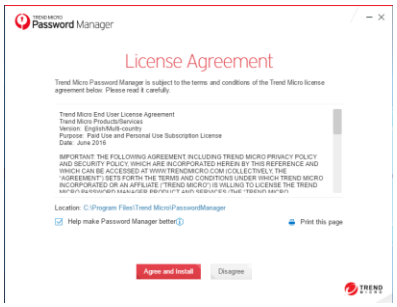



**Figure 297. License Agreement**

10. The installer picks the default location for installation. You can click the link to change the location, but Trend Micro doesn't recommend this.

11. Note the checkbox **Help make Password manager better** is checked by default. This provides technical data to Trend Micro to help improve the product; no personal data is shared. If you wish to opt out of this feedback, uncheck the checkbox.

12. Read the **License Agreement.** If you agree, click **Agree and install.** The installation proceeds and a progress dialog appears, showing you the progress of the installation.

**Figure 298. Password Manager Installation Progress**

13. When the installation is complete, a wizard appears to help you get started.

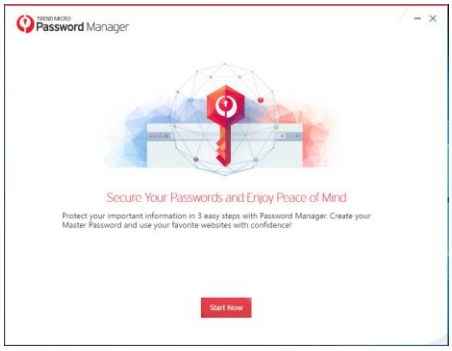



**Figure 299. Start Now**

14. Click **Start Now** to begin the configuration. A window appears in your preferred browser to get the browser extension.

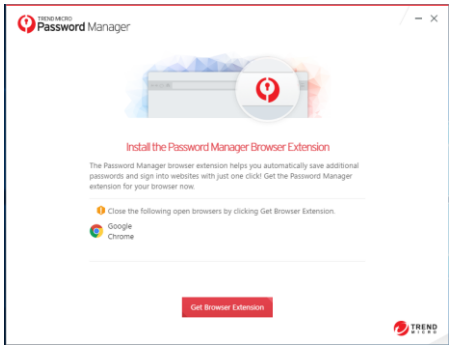



**Figure 300. Get Browser Extension**

15. Click **Get Browser Extension.** This will close your open browser and begin to install the extension.

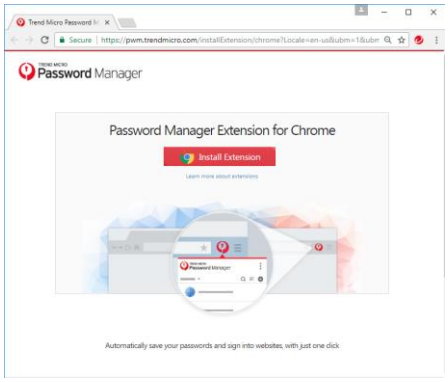



**Figure 301. Install Extension**

16. Click **Install Extension (for Chrome).** A popup appears to add the extension to your browser.

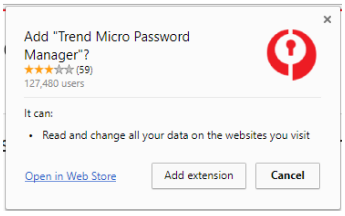



**Figure 302. Add Extension**

17. Click **Add Extension.** The extension is added to your browser.

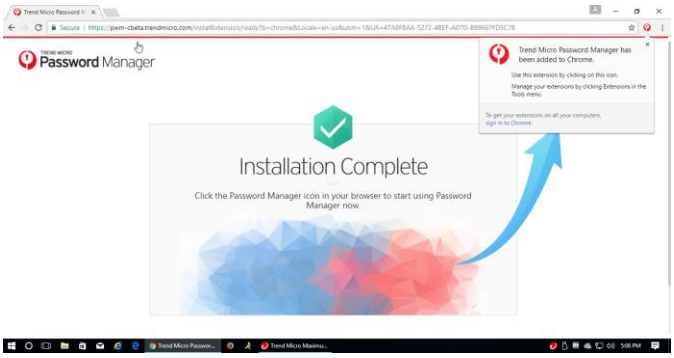



**Figure 303. Installation Complete**

18. When the installation is complete, a screen appears for you to sign into your **Trend Micro Account.**

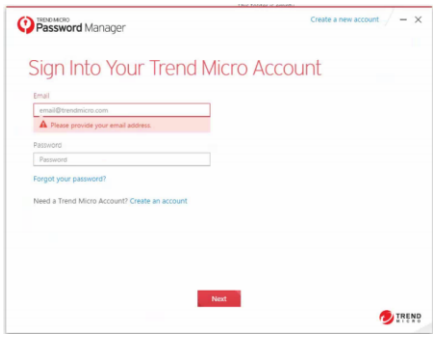



**Figure 304. Sign Into Your Trend Micro Account**

19. Enter the same email address and password you used to register Trend Micro Internet Security (and to create an account) and click **Next**. (This will facilitate your easy upgrade to a **Paid** edition of Password Manager, should you decide to purchase a subscription.) The **Select Your Version screen** appears.

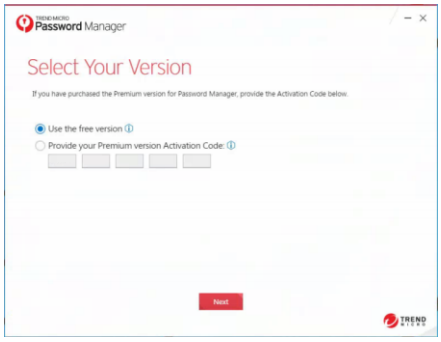



**Figure 305. Use the Free Version**

20. **Use the free version** is selected by default. Click **Next**. The **Protect Your Passwords** screen appears.

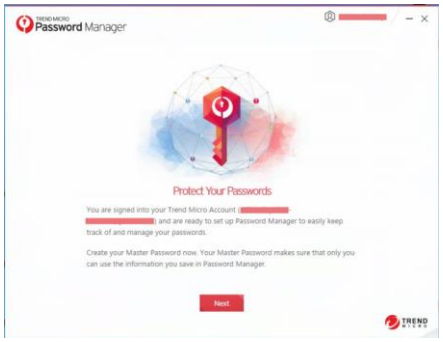



**Figure 306. Protect Your Passwords**

21. Click **Next**. The **Create Your Master Password** screen appears.

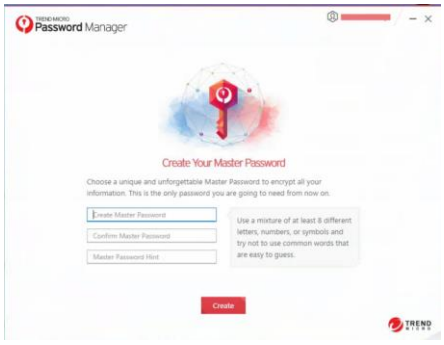



**Figure 307. Create Your Master Password**

22. Use between 6 and 20 characters and at least two kinds of characters among letters, numbers, and symbols.

23. Confirm your **Master Password** and provide yourself a **Password Hint** to help you remember it and click **Create**. You're now ready to start using Password Manager.

24. Click the **Password Manager** icon in your browser. The **Password Manager** popup appears.

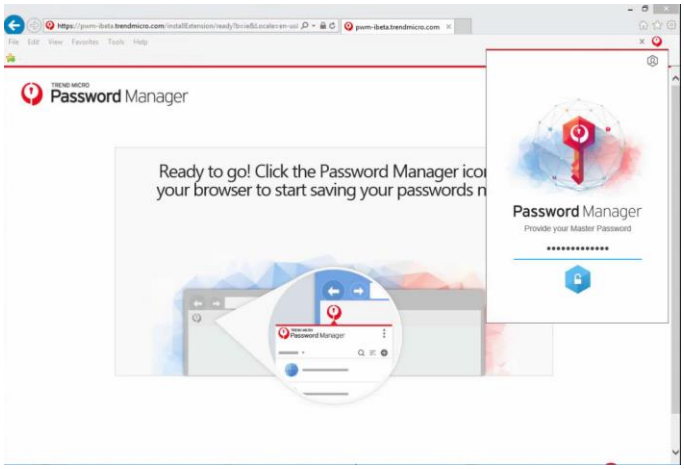



**Figure 308. Provide your Master Password**

25. Enter your **Master Password** and click the **Lock** icon. The **Password Manager** extension opens, with a QR code to download Password Manager to your smartphone.

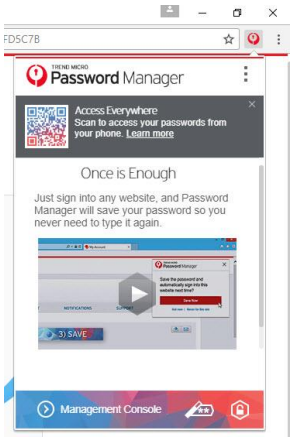



**Figure 309. QR Code**

26. Simply scan the QR Code with a code scanner and it will take you to Google Play or the Apple App Store.
27. Otherwise, simply sign in to any website and Password Manager will save your password—up to 5 passwords for the Free version.
28. For example, go to www.yahoo.com, enter your login ID and password, and sign in.

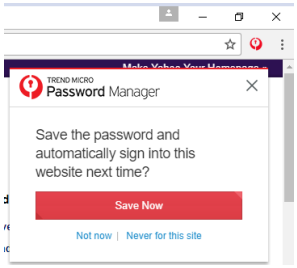



**Figure 310. Save Now**

29. Password Manager captures your login ID and password. Click **Save Now** to save it to Password Manager.
30. In the future, simply go to the same website login page and Password Manager will prompt you to click **Sign In** to sign into your account.

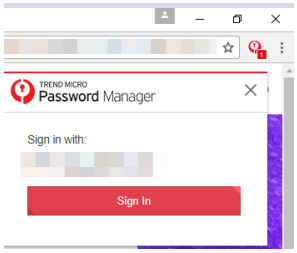



**Figure 311. Sign In**

31. You may also go directly to Password Manager by clicking the Password Manager icon in your browser. This opens your accounts list. Simply click the account listing to take you to the account webpage, where you can click the above **Sign In** button to sign in.

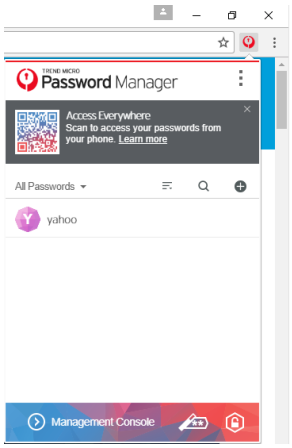



**Figure 312. Yahoo Captured**

32. Repeat the process for up to four additional passwords in the Free version.

**NOTE:** **You can upgrade to a Paid edition of Password Manager at any time and retain your five stored passwords. Upgrading to Trend Micro Maximum or Premium**

**Security will also provide you with a full 1-year subscription to Password Manager.**

33. For full instructions on using **Trend Micro Password Manager**, the *Trend Micro™ Password Manager Product Guide* is available for download from the Trend Micro Support site at Trend Micro Password Manager Support.

# Family: Parental Controls

The **Parental Controls** tool in Trend Micro Internet and Maximum Security lets you protect your children from inappropriate websites, limit their time on the internet, and see detailed reports about what they do online.

To enable **Parental Controls** in Trend Micro Security Internet Security, you first have to enter an email address and password. See the previous section on **Data Theft Prevention** to obtain instructions on doing this.

**Note: The instructions below are tailored to Windows 10 users. The process for creating a new user account in Windows 7 or 8.1 is similar, but not identical.**

**To enable Parental Controls:**

1. Click the **Family** icon in the Trend Micro Security Console. The **Family > Parental Controls** screen appears.

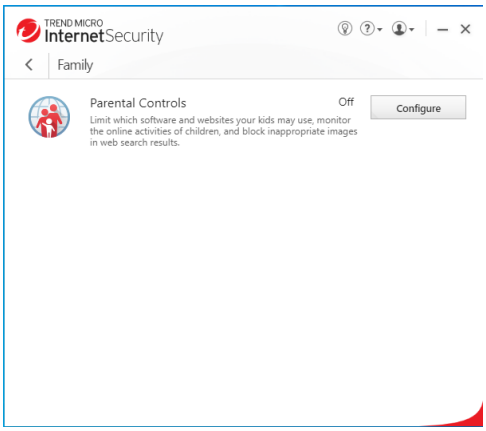



**Figure 313. Family > Parental Controls**

2. Click **Configure**. The **Parental Controls** Introduction screen appears.

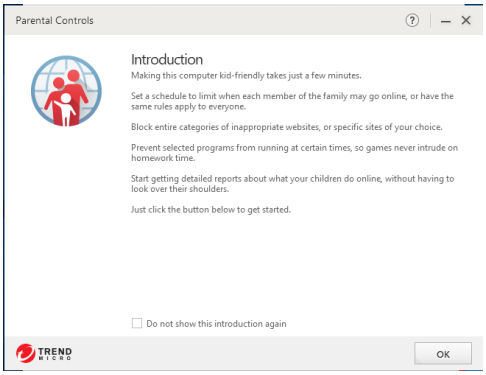



**Figure 314. Parental Controls Introduction**

3. Read the instructions and click **OK** to continue. A screen appears for you to enter your Password.

**Figure 315. Enter Password**

4. Enter your Password and click **OK**. The **Parental Controls Get Started** screen appears.

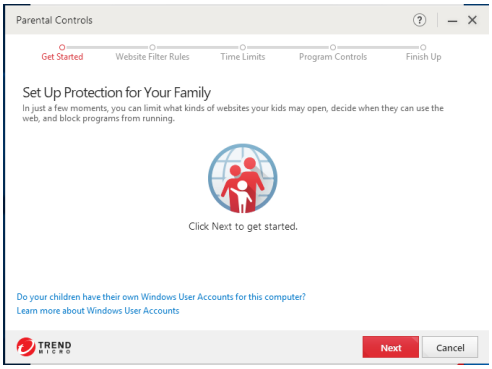



**Figure 316. Parental Controls Get Started**

5. **Important note**: at the bottom of the screen you're asked **Do your children have their own Windows User Accounts for this computer?** If they don't, click the link on the question to create them, so your various settings can be assigned to the proper child. The **Parental Controls > Add Windows Account** screen appears.

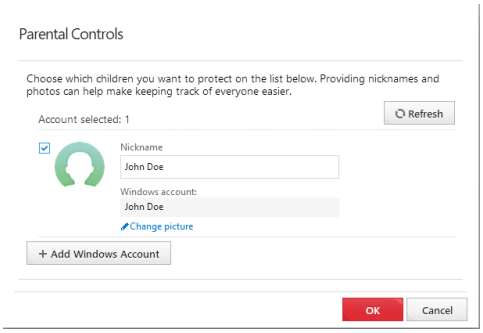



**Figure 317. Parental Controls**

6. In the lower left-hand corner, click **Add Windows Account.** The **User Accounts** Control Panel appears.

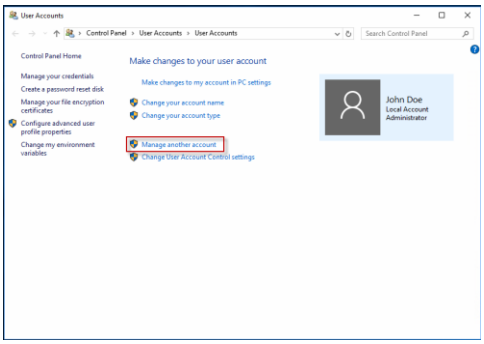



**Figure 318. Windows User Accounts**

7. Click **Manage another account.** The **Manage Accounts** screen appears.

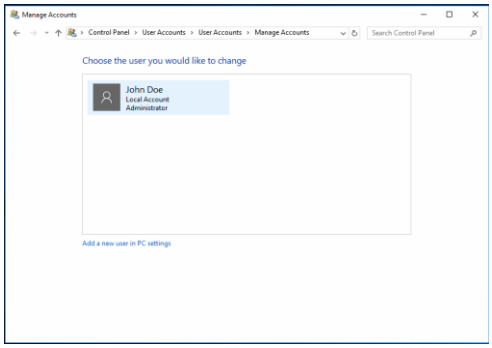



**Figure 319. Manage Accounts**

8. Click **Add a new user in PC settings.** The **Accounts > Family & other users** screen appears.

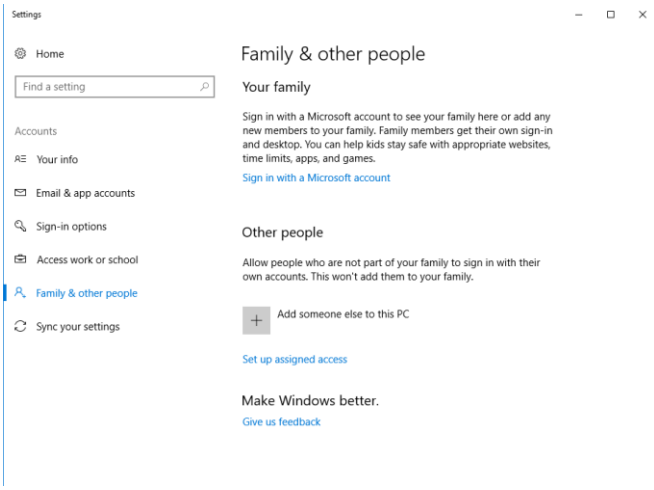



**Figure 320. Accounts > Family & other people**

9. Click **Add someone else to this PC**. A screen appears, asking "How will this person sign in?"

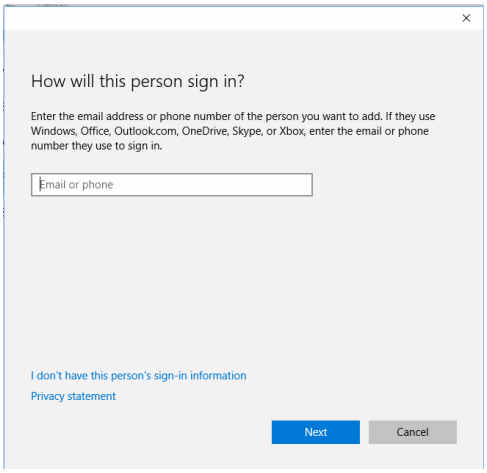



**Figure 321. How will this person sign in?**

10. To simplify this example, we'll start your child without a Microsoft Account. (You can change to a Microsoft Account later.)
11. Click "I don't have this person's sign-in information." A screen appears, prompting "Let's create your account."

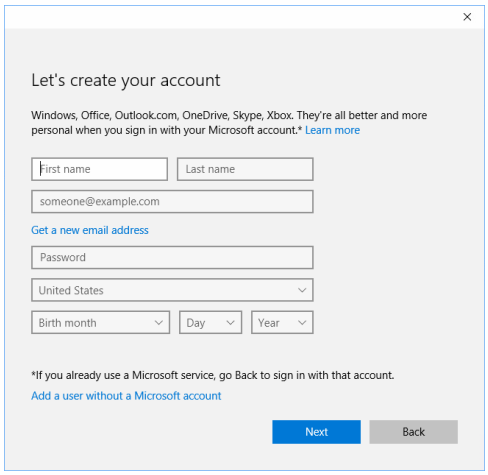



**Figure 322. Let's create your account**

12. Click **Add a user without a Microsoft account.** A screen appears, saying "Create an account for this PC."

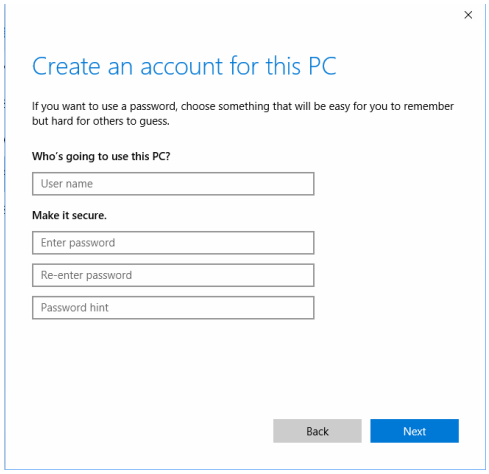



**Figure 323. Create an account for this PC**

13. Type a name for the account (e.g., Mary), enter a password and confirm it, then provide a password hint and click **Next**. The **Accounts > Family & other users** screen appears, confirming the creation of the account for Mary.

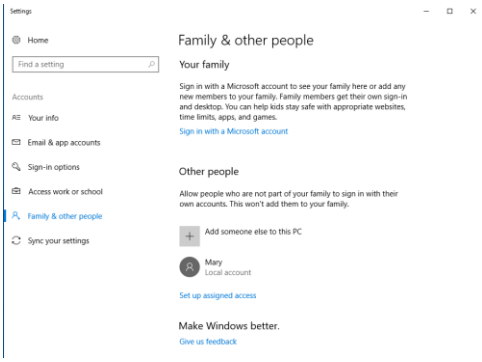



**Figure 324. Local Account created**

14. Back in the **Manage Accounts** screen, you'll see Mary added to the list of accounts on this PC.

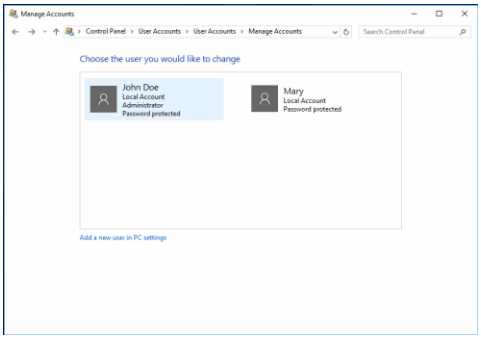



**Figure 325. Local Account - Mary**

15. Close the **Manage Accounts** window by clicking the **Close Box (X)** in the upper-right-hand corner.

16. Back in the **Parental Controls > Add Windows Account** window, click the **Refresh** link if the new account is not showing**.** The **Mary** account now appears in the list.

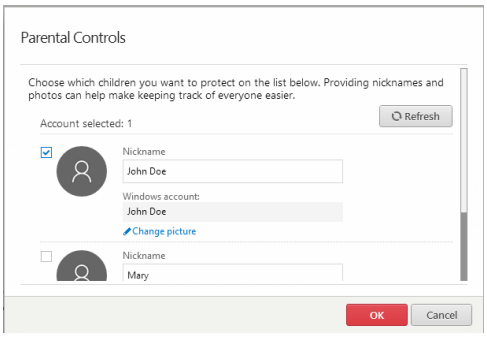



**Figure 326. New Windows Account Listed**

17. Uncheck the account you're logged on to, check the **Mary** account, and click **OK**. A popup appears, telling you "You have not set the rules for one or more users. Let's set it up now."

**Figure 327. Set Up Rules Popup**

18. Click **Ok**. The **Website Filter Rules** window appears.

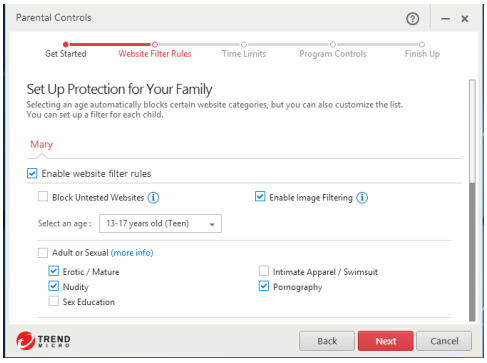



**Figure 328. Website Filter Rules**

19. Check **Block Untested Websites** if you wish. This will block your children from using websites Trend Micro has not tested yet.

20. In the **Select An Age** popup, choose the age the filter will apply to from the **Select an age** pop-up. For example, choose **Ages 3-7 (Child).** (You can also define a **Custom** age bracket.)

    For a child this age, all categories and subcategories are checked. Scroll down to see the full category/subcategory listings.

    You can check or uncheck a category or subcategory to redefine the filter. You can also obtain more information on a category by clicking the **more info** link; a definition list will pop up.

21. Click **Next** to define the **Time Limits.** The **Time Limits** window appears.

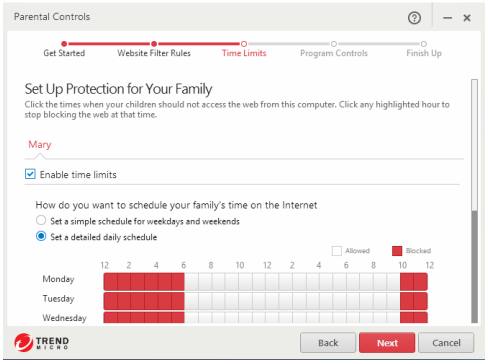



**Figure 329. Time Limits**

22. Using your mouse pointer, select the weekday and weekend hours you kids **should not** access the web by holding your mouse down and stroking across the hours, then scroll down and indicate the number of hours your children may use this computer.

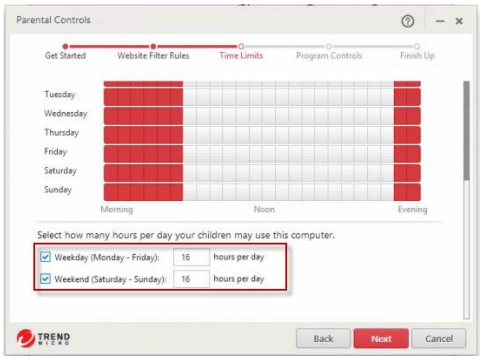



**Figure 330. Allowed Hours on Computer**

23. Upwards in the window you may also **Set a simple schedule for weekdays and weekends**, applying the same schedule across all days at once.

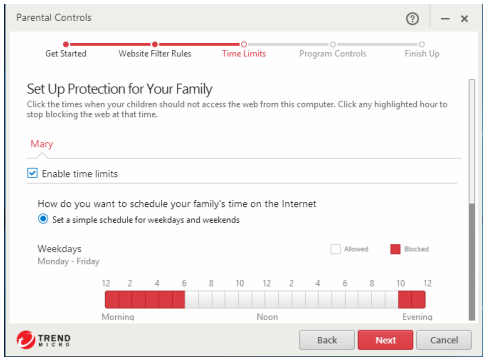



**Figure 331. Detailed Daily Schedule**

24. Click **Next**. A screen appears, letting you set the child's program controls.

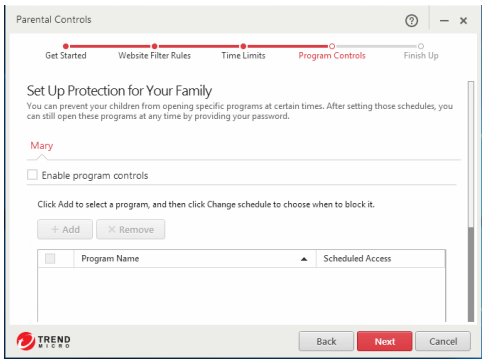



**Figure 332. Program Controls**

25. Check **Enable program controls**, then click **Add** to add the programs you want to control the usage of.

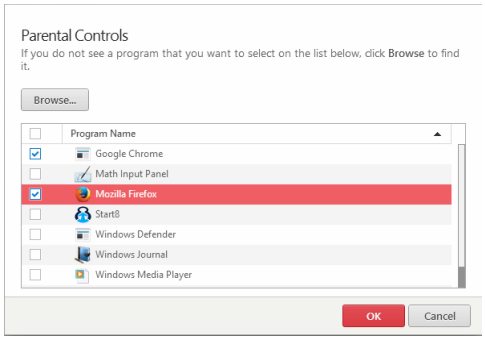



**Figure 333. Program List**

26. Select the program you want to control from the list, or click **Browse** to find it.

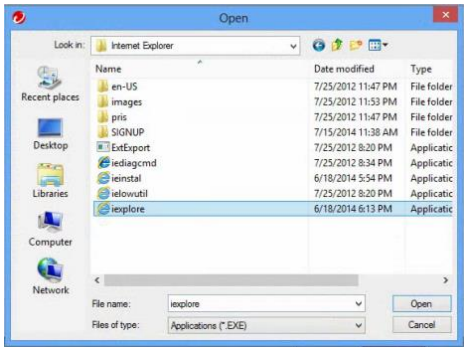



**Figure 334. Browsing for Programs to Add to Program Controls**

27. Navigate to the program in the **Programs Folder**, select it from its own folder (e.g., Internet Explorer), and click **Open**. Trend Micro Security adds it to the list of controlled programs.

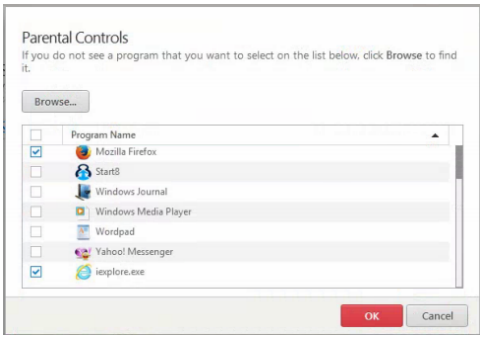



**Figure 335. Programs in List | IE Added**

28. Check the program checkbox and click **OK**.

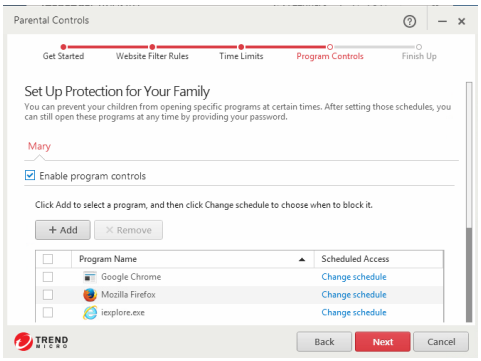



**Figure 336. Change Schedule**

29. The program is added to the **Parental Controls** window. You can now set the times the program may be used. Click **Change Schedule** in the **Scheduled Access** field. The schedule appears.

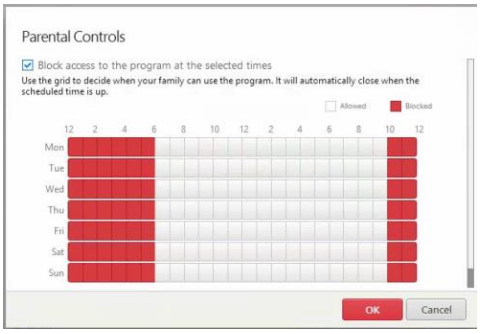



**Figure 337. Access Schedule**

30. **Block access to the program at the selected times** and **all hours** are selected by default. *Deselect* the hours in the week the child will be permitted use of the program, then click **OK**. When the wizard window appears, click **Next**.

31. A screen appears, indicating that protection has been activated for **Mary**, applying the **Pre-teen Website Filter**, giving the **Time Limits** and **Program Controls**.

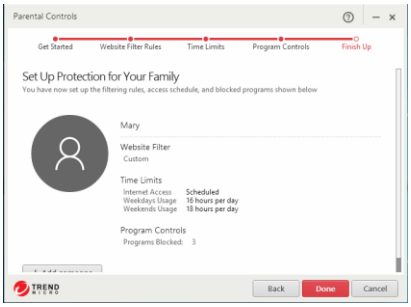



**Figure 338. "Mary" Protection Criteria**

32. Click **Done** to finish adding the parental control for this child. The main **Parental Controls** window reappears.

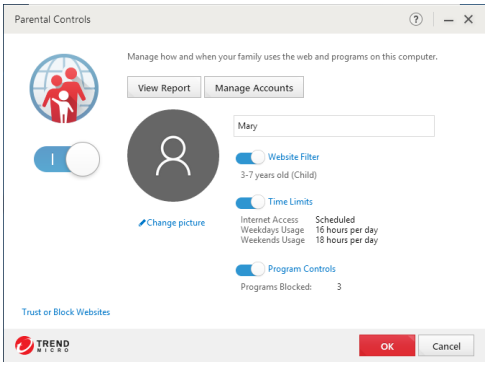



**Figure 339. Sliders are "On"**

33. In **Parental Controls,** the slider buttons should be **On**. If not, slide to **On**, then click **OK**. The rule set is now applied to the **Mary** account.

34. Note that the link **Trust or Block Websites** allows you to set exceptions to your rules. This function was covered in the previous **Trend Micro Antivirus+ Security** section. Go to Exception Lists: Websites for details.

35. Note also that you can turn the **Website Filter**, **Time Limits,** and **Program Controls** functions on or off by using the appropriate slider. You can also edit the functions by clicking the hotlinks and making your changes in the respective editor.

36. Click **OK** to close the **Parental Controls** window, then click the respective **Close** boxes to close the **Parental Controls** window and the **Trend Micro Security Console.**

37. In the Windows Menu, select **John Doe**, then select **Mary** to switch to her account; then sign in using the password you created for her account.

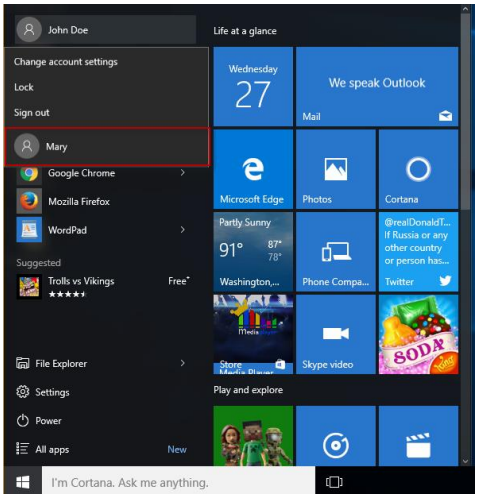



**Figure 340. Switching to "Mary" Account**

**Figure 341. Mary Login**

38. Using your browser, attempt to go to a website at a time prohibited by the account rules. Trend Micro Security will block access to the web and provide a **No Web Surfing Allowed** notification, indicating the user cannot use the web at this time.

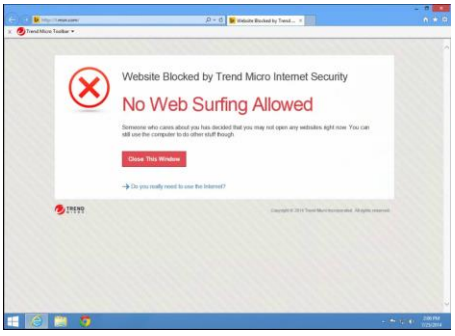



**Figure 342. No Web Surfing Allowed**

39. During the hours allowed for surfing, if the user attempts to browse to a site not permitted by the rules, Trend Micro Security will block access to the site and provide an **Off Limits** notification for the user in the browser.

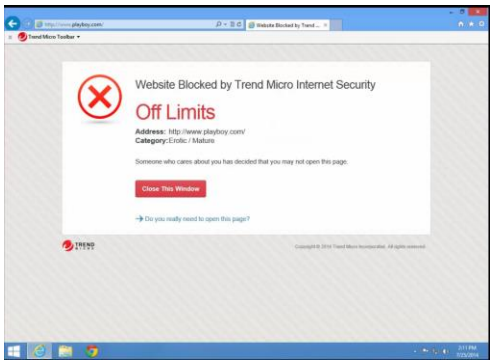



**Figure 343. Trend Micro Security Off Limits Notification in Browser**

40. Finally, if the user tries to use a blocked program during the hours you've chosen to block it, a popup appears saying **Program Accessed Blocked.**

**Figure 344. Program Access Blocked**

41. If the user knows the Trend Micro Security password on the computer, they can override the block. Naturally, for their own safety, kids being monitored should not be given access to this password.

## Security Report: Parental Controls

Once you've enabled Parental Controls, Trend Micro Security Internet Security provides a security report that can give you basic information about how many times your kids have attempted to access prohibited sites and the kinds of website violations they are.

**To view the Parental Controls Security Report:**

1. Open the Trend Micro Security Console.

**Figure 345. Console > Security Report**

2. Click the **Security Report** icon. The **Password** popup appears.

**Figure 346. Password Screen**

3. Enter your password and click **OK**. The **Security Report** window appears, with **Security Threats** selected by default.

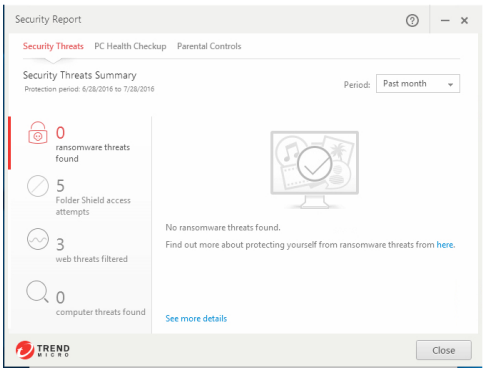



**Figure 347. Security Reports > Security Threats**

4. Click the **Parental Controls** tab to show the **Parental Controls Security Report**. The **Parental Controls Security Report** appears.

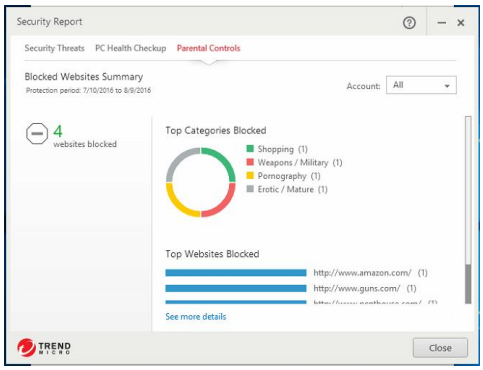



**Figure 348. Parental Controls Security Report**

5. The report will show the **Top Categories** and **Websites Blocked.** Use the **Account** pop-up to show the report for **All users**, or for a specific user account; e.g., "Mary."

**Note:** **The administrator will receive a monthly Security Report via email, which includes Parental Controls data.**

6. Click **See More Details**, to display the **Parental Controls** log.

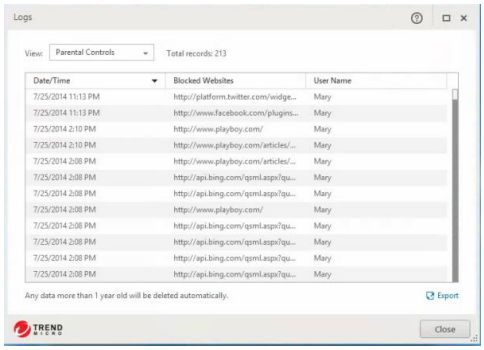



**Figure 349. Parental Controls Logs**

7. Note that any data older than a year ago will be deleted automatically.

8. Click **Export** to export the Parental Controls log in .CSV or .TXT format.

# Chapter 6: Trend Micro Maximum Security

This chapter provides detailed instructions for configuring and using Trend Micro Maximum Security. The Maximum edition provides everything previously described in the Trend Micro Security Antivirus+ and Internet Security chapters, while adding more protections and tools.

## Protection Overview

**Trend Micro Maximum Security** is functionally the most robust edition of Trend Micro Security. To enable all its functions, you need a paid version of Trend Micro Maximum Security.

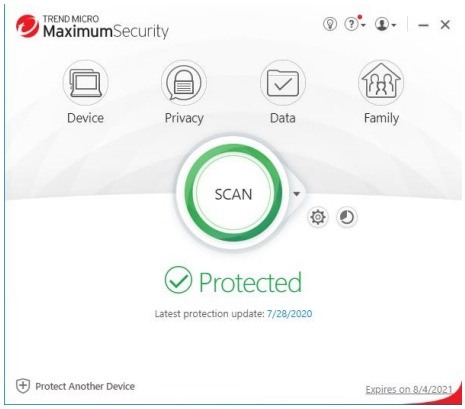



**Figure 350. Trend Micro Maximum Security Console**

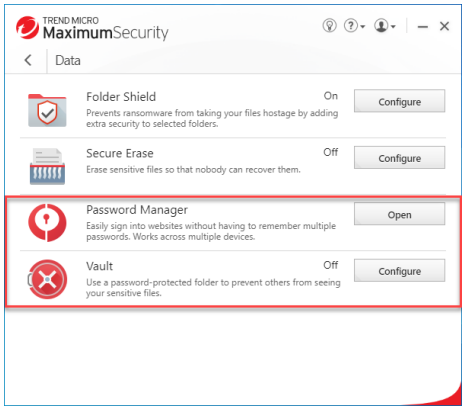



**Figure 351. Data > Password Manager | Vault**

**Note:** **Trend Micro Maximum Security's Additional Features:**

**Data: Password Manager (auto-installed) and Vault.**

**Additional Seats: Trend Micro Security Maximum users can protect from five to ten devices, depending on the purchase level, choosing among PC, Mac, Android, and iOS devices.**

**ADDITIONAL TOOLS FOR TREND MICRO SECURITY MAXIMUM SECURITY PAID VERSION**

**Password Manager – Auto-installed**

Your installation of Trend Micro Maximum or Premium Security also auto-installs a copy of Trend Micro Password Manager onto your computer. Using Password Manager, you can easily sign into websites without having to remember multiple passwords. Generate strong passwords that are harder to crack and replace weak ones that you're using because they're easy to remember. Use the Secure Browser to access banking and other financial sites, to protect yourself against keyloggers.

**Vault**

Users can enable a password-protected folder that can secure sensitive files. If the computer is lost or stolen, the vault can be sealed shut by remote control until the computer is returned to its rightful owner.

## Device: Protect Another Device

Trend Micro Maximum Security provides a subscription for five to ten devices, depending on the subscription, across Windows, Mac, Android, and iOS devices.

Go to **Protect Another Device: PCs, Macs, Android and iOS Mobile Devices** for more details.

## Data: Password Manager - Full Version

**Trend Micro™ Password Manager** helps you manage and secure all your online credentials, ensuring an easy and safe online experience, while offering a faster, more secure, and convenient way to access web sites. Using a single Master Password, users have instant access to all their login credentials, no matter where they're located or what device they're using.

A full 1-year subscription of Password Manager is auto-installed with Trend Micro Maximum Security. You can opt out of the auto-installation.

**To Start Using Password Manager:**

**Note:** **The instructions below assume you registered Trend Micro Maximum Security when you installed it, that you created a Trend Micro Account during activation, and that you're signed in.**

1. Open the **Trend Micro Security Console** and click the **Data** icon. The **Data** screen appears.

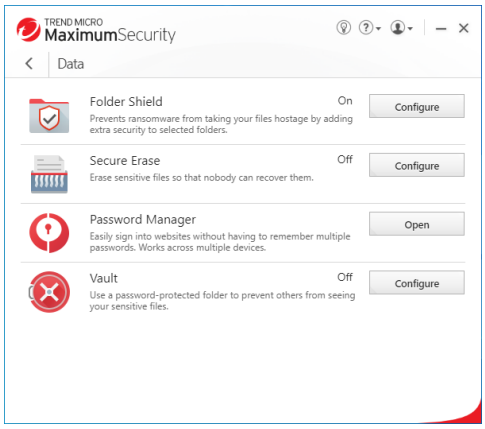



**Figure 352. Data > Password Manager > Open**

2. Click **Open** in the **Password Manager** panel. The **Password Manager Introduction** screen appears.

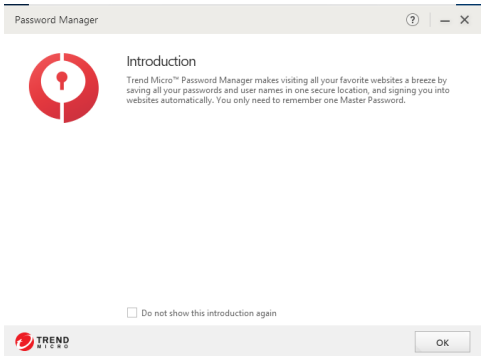



**Figure 353. Password Manager Introduction**

3. You may check "Do not show this introduction again" if you choose, then click **OK** to close the introduction. A screen appears to **Secure Your Passwords and Enjoy Peace of Mind.**

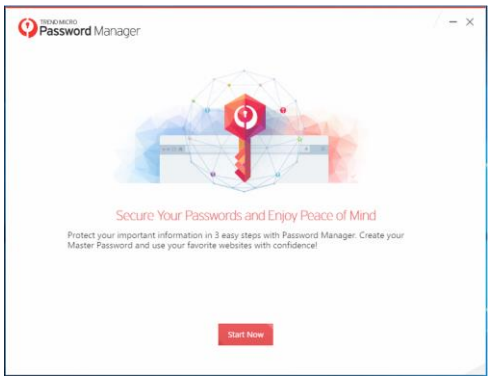



**Figure 354. Secure Your Passwords and Enjoy Peace of Mind**

4. Click **Start Now.** A screen appears for you to **Install the Password Manager Browser Extension.**

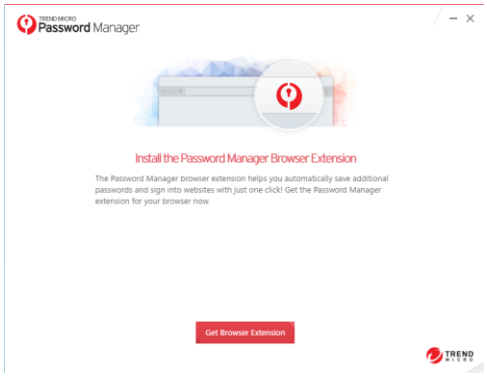



**Figure 355. Install the Password Manager Browser Extension**

5. Click **Get Browser Extension.** A screen appears to **Protect Your Passwords with Password Manager.** A browser window appears for you to install the extension in your default browser; e.g., Chrome.

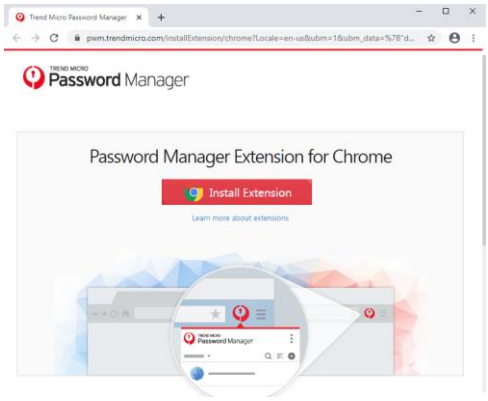



**Figure 356. Password Manager Extension for Chrome**

6. Click **Install Extension.** In this example, the **Chrome Web Store** loads in your Chrome browser.

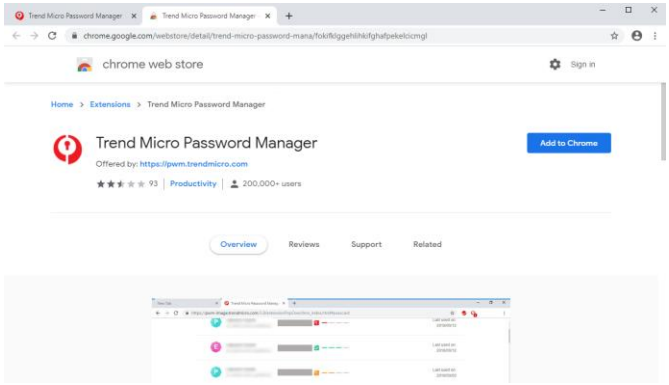



**Figure 357. Chrome Web Store - Trend Micro Password Manager**

7. Click **Add to Chrome.** A popup appears, asking you to **Add "Trend Micro Password Manager"?**

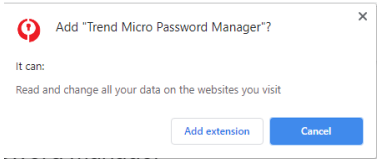



**Figure 358. Add "Trend Micro Password Manager"?**

8. Click **Add Extension.** A popup appears, indicating Trend Micro Password Manager has been added to Chrome.

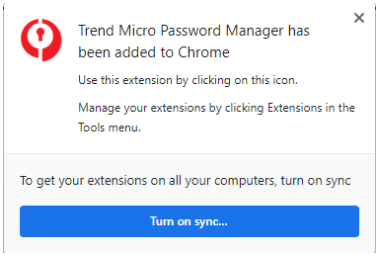



**Figure 359. Trend Micro Password Manager Added to Chrome**

9. You may Turn on sync… if you wish by logging into your Google account. For now, click the **Close (x)** box. The **Add Ons** icon appears in Chrome.

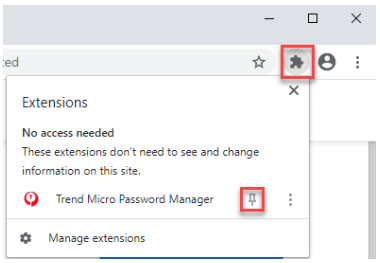



**Figure 360. Pin Password Manager to the Chrome Menu**

10. Click the **Add Ons** icon, then click the **Pin** icon to pin the **Password Manager** extension to the Chrome menu. The icon appears.

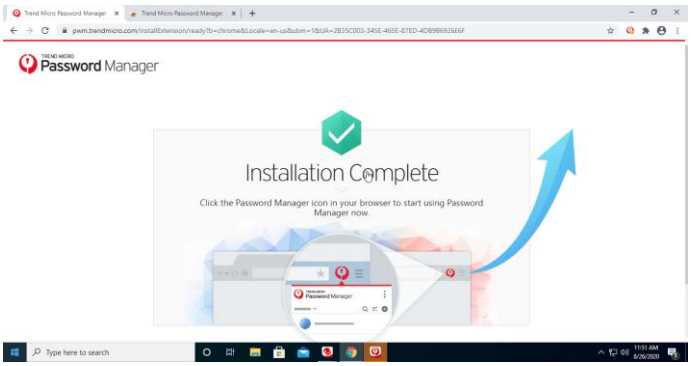



**Figure 361. Password Manager Installation Complete**

11. Your browser indicates **Installation Complete.** You now need to create a Master Password to begin using Password Manager.

12. Click the **Password Manager** icon in your browser. The **Password Manager** drop-down menu appears.

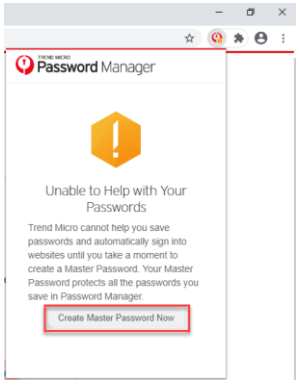
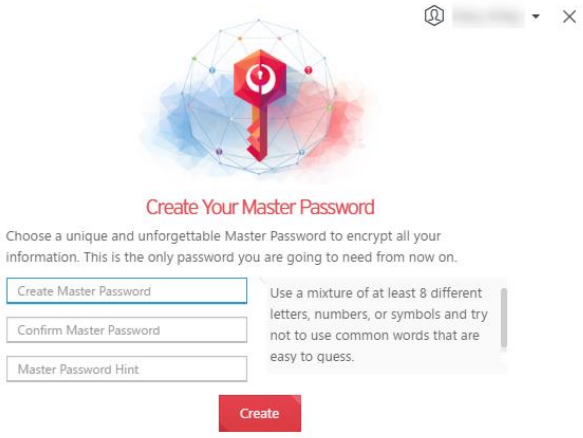
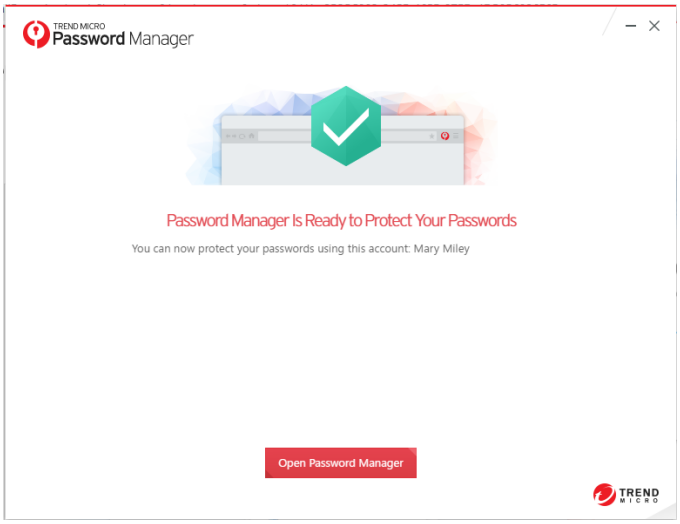



**Figure 362. Create Master Password**

13. Click **Create Master Password Now**. A screen appears for you to **Create Your Master Password.**




14. Create your **Master Password**, **Confirm** it, and provide yourself a **Master Password Hint**. Use a mixture of at least 8 different letters, numbers, or symbols and try not to use common words that are easy to guess.
15. Click **Create** and a screen appears indicating that **Password Manager is Ready to Protect Your Passwords.**




16. Click **Open Password Manager** to open the **Management Console**, or click the **Password Manager** icon to show the **Extension** drop-down menu.

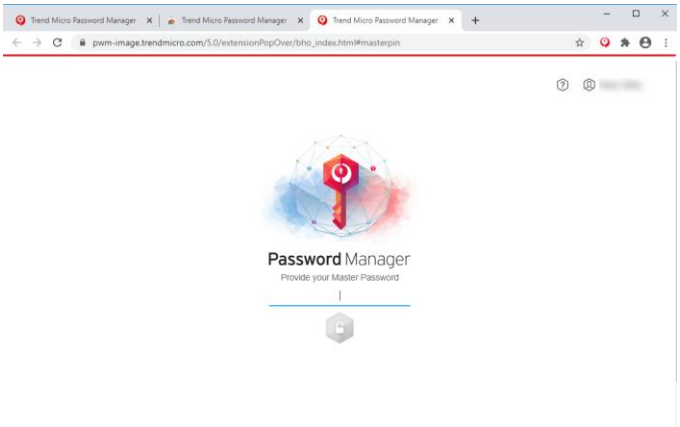



**Figure 363. Password Manager Management Console (1)**

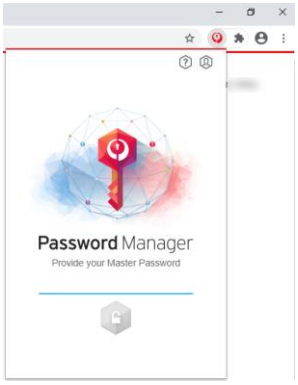



**Figure 364. Password Manager Extension**

17. Either way, provide your **Master Password**, then click the **Unlock** icon to log in. Password Manager opens and is ready to capture your passwords.

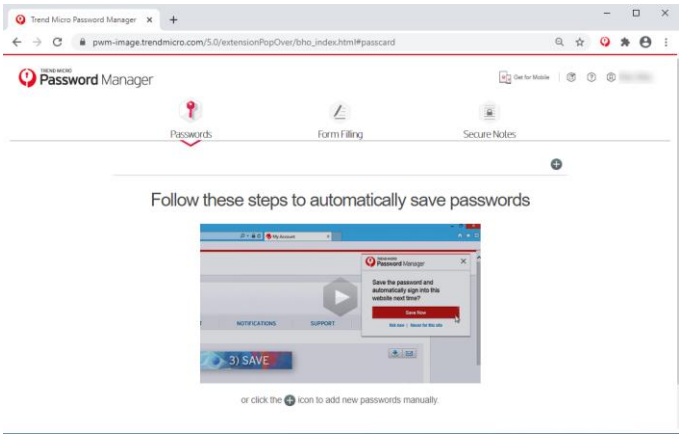



**Figure 365. Password Manager Management Console (2)**

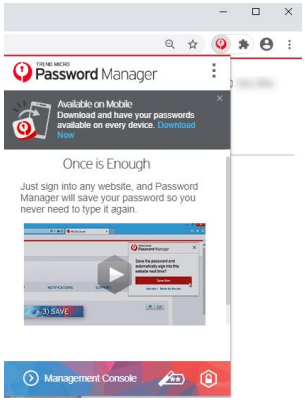



**Figure 366. Password Manager Extension**

18. Watch the video to learn how to capture your passwords, or simply log into your accounts and **Password Manager** will automatically capture your credentials. It will then automatically play them back the next time you log into the account.

## Install Password Manager in Pay Guard

**To Install Password Manager in Pay Guard:**

1. Once you've activated your **Trend Micro Password Manager** account as given above, you may also install **Password Manager** in **Pay Guard**.
2. Double-click the **Pay Guard** icon on your Desktop. The **Pay Guard** window appears, with a popup window suggesting **Add the Password Manager extension to Pay Guard to access your passwords. Browser will restart)**

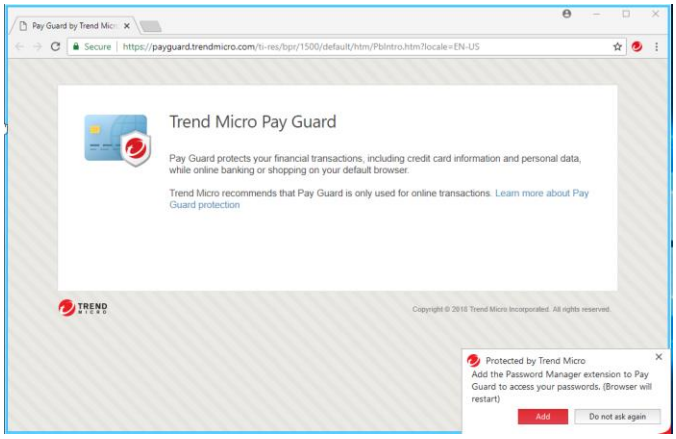



**Figure 367. Pay Guard > Install Password Manager**

3. Click **Add** to add the Password Manager extension. A window opens for you to install the extension.

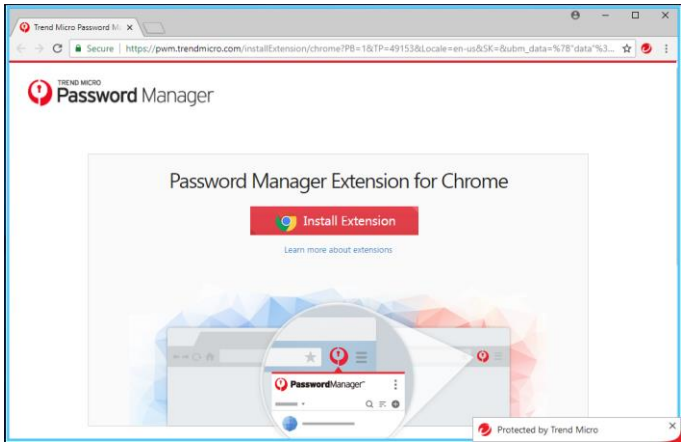



**Figure 368. Install Extension**

4. Click **Install Extension.** In our example, since Chrome is the default browser, you're taken to the Chrome store to install the extension.

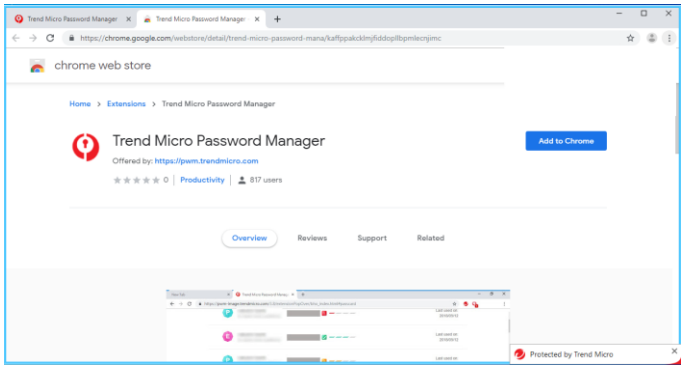



**Figure 369. Add Password Manager**

5. Click **Add to Chrome.** A popup appears, asking **Add "Trend Micro Password Manager"?**

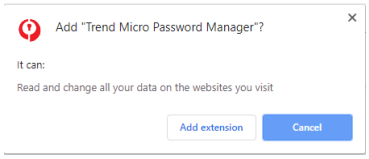



**Figure 370. Add Extension**

6. Click the **Add extension** button. The **Password Manager** extension installs and reboots your **Pay Guard** browser, showing **Installation Complete.**

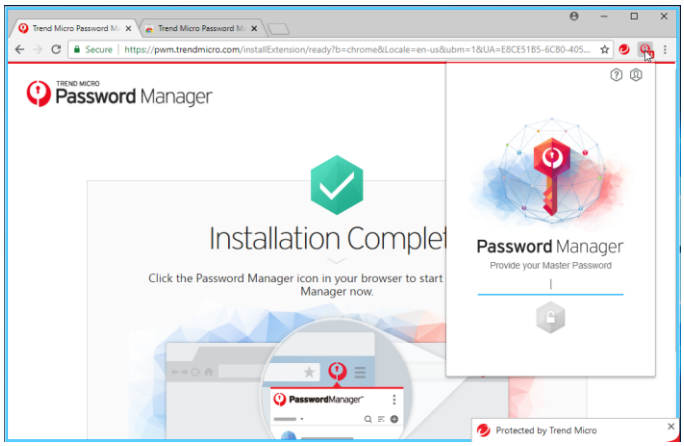



**Figure 371. Installation Complete**

7. You're now ready to use Password Manager in your full default browser or in **Pay Guard.**

## Using Password Manager

**To Use Password Manager:**

1. Using your default browser or **Pay Guard**, simply sign in to any website and **Password Manager** will save your password.
2. For example, go to www.yahoo.com, enter your login ID and password, and sign in.

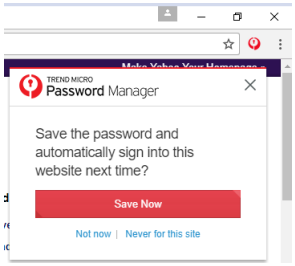



**Figure 372. Save Now**

3. Password Manager captures your login ID and password. Click **Save Now** to save it to Password Manager.
4. In the future, simply go to the same website login page and Password Manager will prompt you to click **Sign In** to sign into your account.

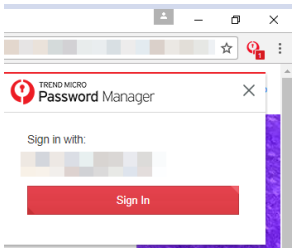



**Figure 373. Sign In**

5. You may also go directly to Password Manager by clicking the Password Manager icon in your browser. This opens your accounts list. Simply click the account listing to take you to the account webpage, where you can click the above **Sign In** button to sign in.

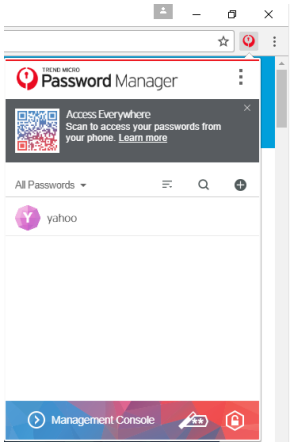



**Figure 374. Yahoo Captured**

6. Log off **Password Manager** by clicking the **Lock** icon in the lower right-hand corner of the **Password Manager** popup. That's it! You now know how to capture and use passwords in **Password Manager**.

7. For full instructions on using **Trend Micro Password Manager**, the *Trend Micro™ Password Manager Product Guide* is available for download from the Trend Micro Support site at Trend Micro Password Manager Support, then click on the Windows, Mac, Android, or iOS tabs for the platform(s) you're interested in.

# Data: Vault

**Vault** is a password-protected folder that can protect your sensitive files. Using a password, files inside the Vault are kept invisible until you enter the password. If your computer is stolen, Vault can also seal itself shut by remote control, so that even using the password you cannot open the Vault—that is, until the computer is returned to its rightful owner, who then must report that the computer has been found.

**To set up Vault:**

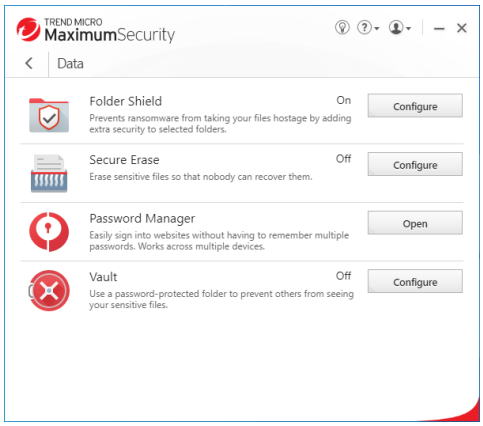



**Figure 375. Data > Vault > Configure**

1. In the Trend Micro Security Console, click the **Data** icon, then **Configure** in the **Vault** panel. The **Introduction** to **Vault** appears.

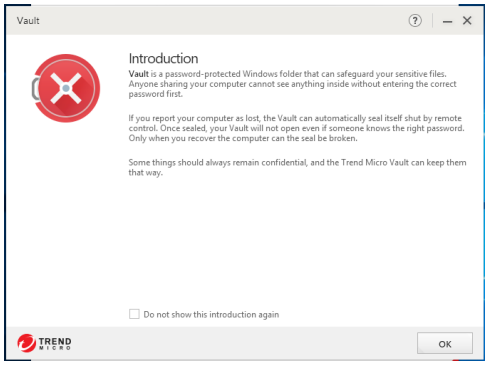



**Figure 376. Data > Introduction to Vault**

2. Click **OK** to close the Introduction. The **Select a Password** screen appears.

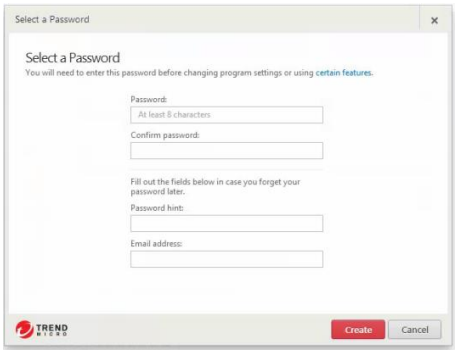



**Figure 377. Select a Password**

3. Enter a password and confirm it, then provide a hint and your email address and click **Create**. A setup dialog appears, telling you that you have successfully set up the **Vault** and to double-click its desktop icon to start using it.

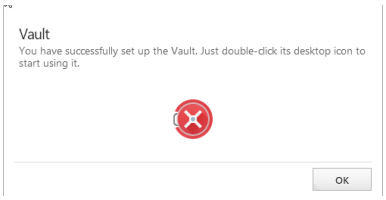



**Figure 378. Vault Set Up**

4. Click **OK** to close the dialog. The **Vault** window appears, with the slider turned to **On**, and instructions on reporting a loss and regaining access to the **Vault**.

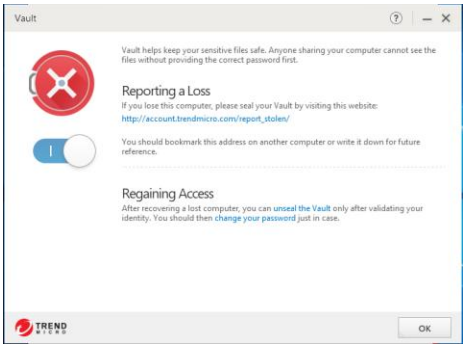



**Figure 379. Vault**

5. The **Vault** desktop icon also appears on your desktop.

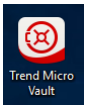



**Figure 380. Vault Desktop Icon**

6. You can now use the **Vault** to protect your sensitive files, to seal the vault if your computer is stolen or misplaced, and to regain access to the vault if you've turned it off.

7. To open the **Vault**, double-click the desktop icon. The password window appears.

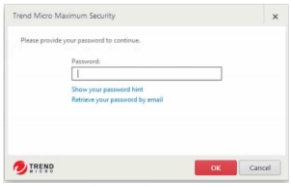



**Figure 381. Vault > Password Protection**

8. Enter your password and click **OK**. This opens the **Vault.**

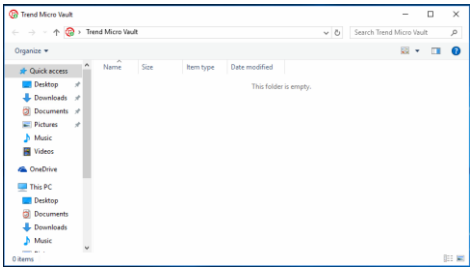



**Figure 382. Trend Micro Vault**

9. Drag files and folders you wish to protect into the **Vault**, then close it.

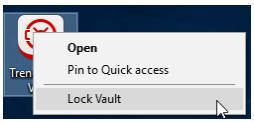



**Figure 383. Lock Vault Menu Item**

10. Right-click the **Vault** and select **Lock Vault** to lock it. A dialog appears, warning you that locking the vault does not automatically block access to files currently open. Make sure you close all files that need protection before you lock the Vault.

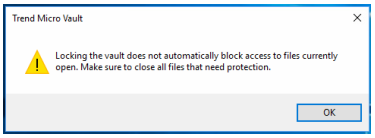



**Figure 384. Trend Micro Vault Warning**

11. Click **OK** to close the dialog.

12. In the Trend Micro Console Vault window, note the link http://account.trendmicro.com/report_stolen/ for reporting a loss.

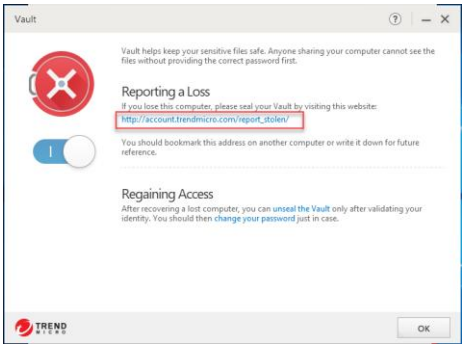



**Figure 385. Reporting a Loss**

13. You should bookmark this link on another computer or write it down for future reference. Clicking it takes you to the Trend Micro Vault **Report Stolen** webpage, where you can report the loss.

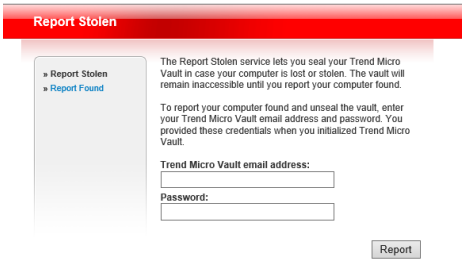



**Figure 386. Report Stolen Service**

14. In the **Report Stolen** webpage, enter your Trend Micro Vault email address and password and click **Report** to seal the vault. Once you do, your Vault-protected folders and files cannot be opened.

15. Once you recover the computer, open the Trend Micro Security console, click **Data > Trend Micro Vault**, re-enter your password, then click the link **Unseal the Trend Micro Vault** in the **Regaining Access** paragraph.

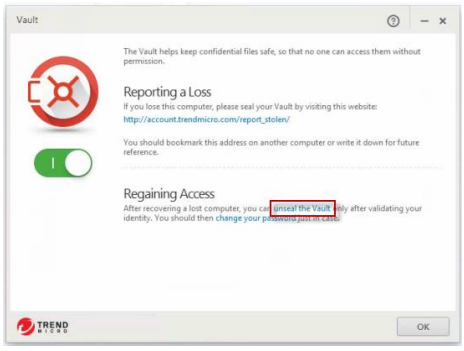



**Figure 387. Regaining Access**

16. This takes you to the Trend Micro Vault Report **Report Found** webpage, where you can unseal the Vault.

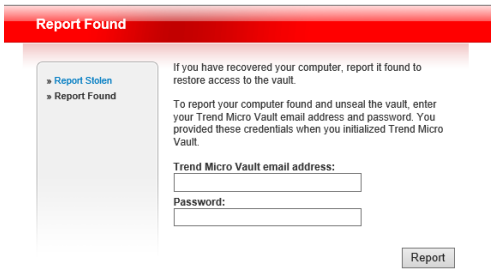



**Figure 388. Report Found**

17. Enter the **Trend Micro Vault email address** and **Password** and click **Report**. This unseals the Vault and you're notified by Trend Micro Security.
18. For your safety, you should now change your Trend Micro Security password.

# Chapter 7: Trend Micro Security: Explore More Features, Get Help, Identity, and Tools

All Trend Micro Security editions provide **Explore More Features, Help, and Identity** menus in the **Console**.

## Explore More Features

**To Explore More Features:**

**Figure 389. Explore More Features Icon**

1. Click the **Lightbulb – Explore More Features** icon in the **Console**. A questionnaire appears.

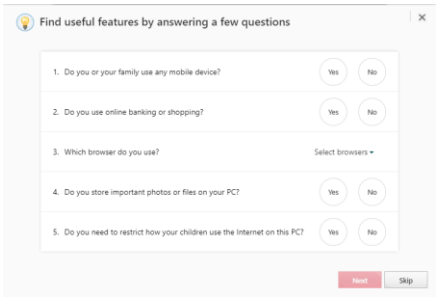



**Figure 390. Questionnaire**

2. Click the respective **Yes/No** icons and choose the browser drop-down menu to tailor the wizard's replies.

   Go to **Explore More Features – Questionnaire and Wizard** for more details.

# Help > Product Support

**To get Help (?) > Product Support:**

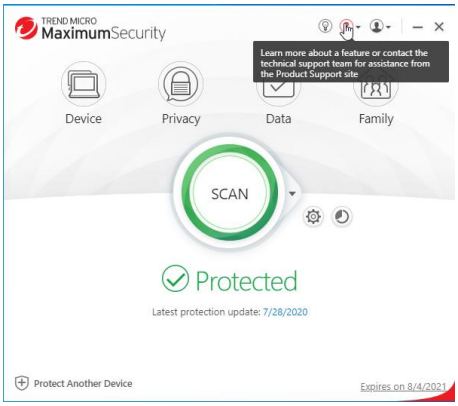



**Figure 391. ? (Help)**

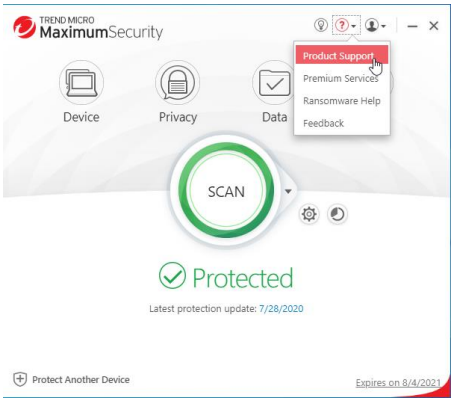



**Figure 392. Get Help**

3. Click **? (Help)** in the Console, then choose **Product Support** in the drop-down menu. The **Product Support** page appears.

**Figure 393. Trend Micro Maximum Security Support (image subject to change)**

4. Here you can get access to training videos, this product guide, and a wide range of support topics to help you get the most out of your security software. Use the drop-down menus for **Support Topics** and **Related Product Support** to obtain relevant information, or click the **Discussion Forums** link for the latest discussion and support.

# Help > Premium Services

**To access Premium Services:**

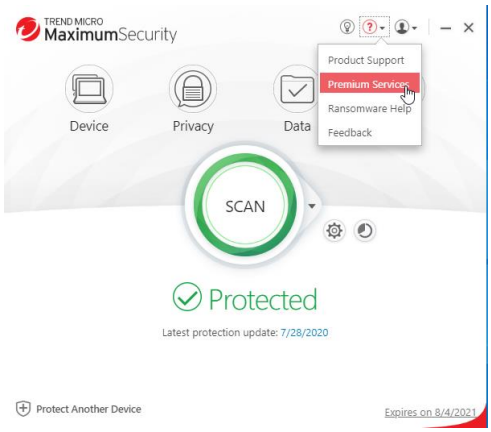



**Figure 394. ? (Help) > Premium Services**

1. Choose **Premium Services** in the **? (Help)** menu. The **Premium Services for Home Users** webpage appears.

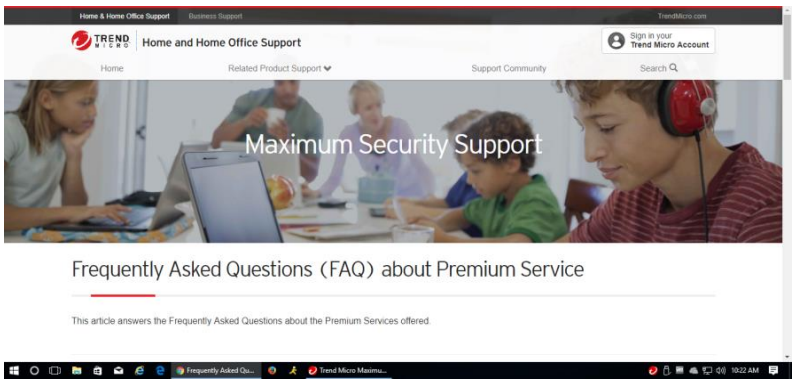



**Figure 395. Premium Service (image subject to change)**

2. Here you can obtain answers to frequently asked questions about Premium Service and to purchase a plan to enable a Trend Micro technician to make a “virtual house call” any time, day or night, to help you with any problems you may have with your computer.
3. Select the region you inhabit for the correct plan and pricing.

# Help > Ransomware Help

**To get help with ransomware:**

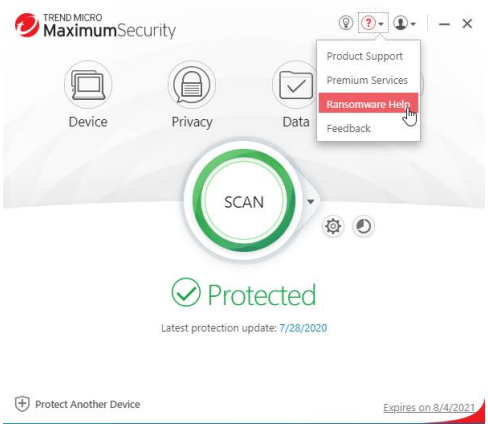



**Figure 396. Ransomware Help**

1. Choose **Ransomware Help** in the **? (Help)** menu. The **Ransomware Help** webpage appears.

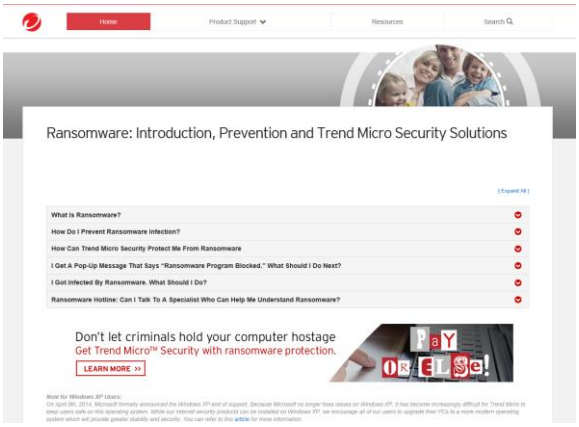



**Figure 397. Ransomware Help Webpage (Image subject to change)**

2. Here you can get information on ransomware, including advice on what to do if you're under a ransomware attack. See the **Ransomware Hotline** entry for information on getting live help from a Trend Micro Support Specialist.

# Help > Feedback

**To Provide Feedback:**

1. Open the **Trend Micro Security Console** and click the **Help (?) Menu**. A drop-down menu appears.

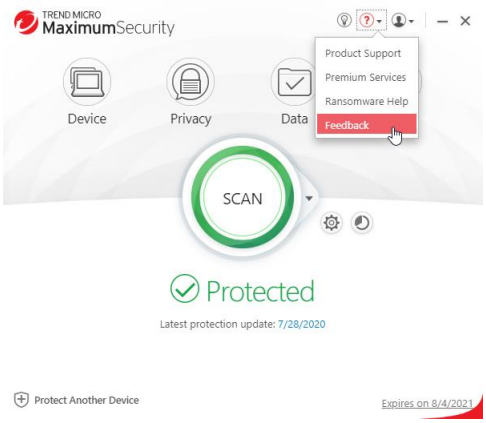



**Figure 398. Feedback**

2. Choose **Feedback** in the drop-down menu. The **Trend Micro Home Users Community Forum** page appears for **Desktop Protection > PC Security.**

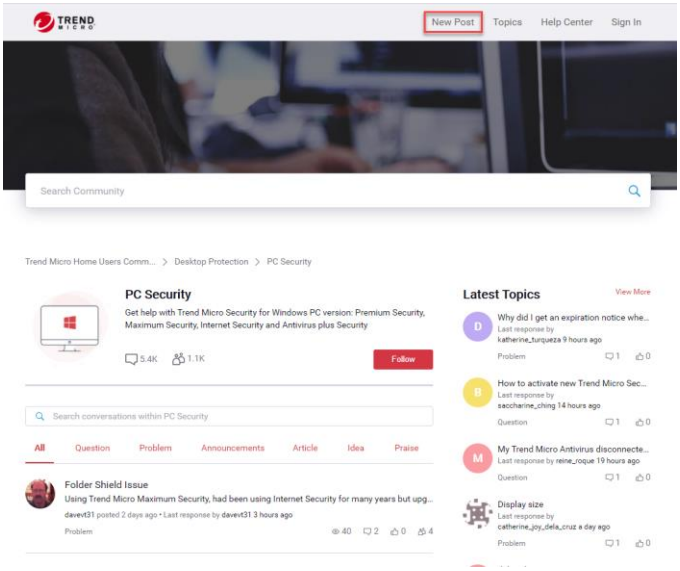



**Figure 399. Trend Micro Home Users Community Forum**

3. Click **New Post.** The **Posting** page appears.

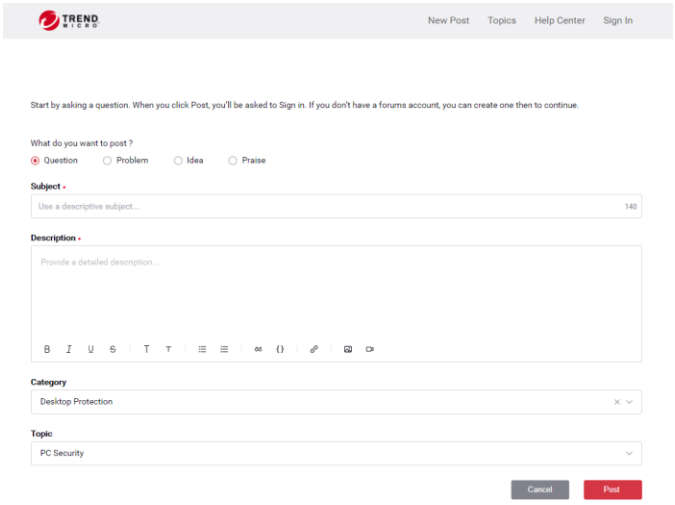



**Figure 400. Posting Page**

4. Select the button to ask a **Question**, report a **Problem**, share an **Idea**, or just give some **Praise**; then enter a **Subject**, provide a **Description**, use the drop-downs to choose a **Category** and **Topic**, then click **Post**. If you don't have a **Forum** account you can create one to continue.
5. After your post, return to the **Forum** to see your post and any responses from users or developers.

# ID > Account

**To check your Account:**

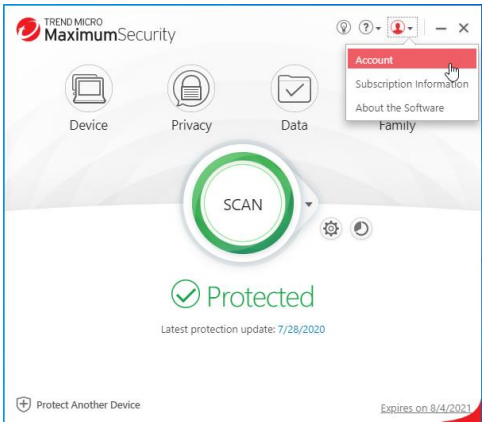



**Figure 401. Account**

1. Click the **ID** (**Identity)** menu, then choose the **Account** menu item in the Console. The **Trend Micro Account** webpage appears.

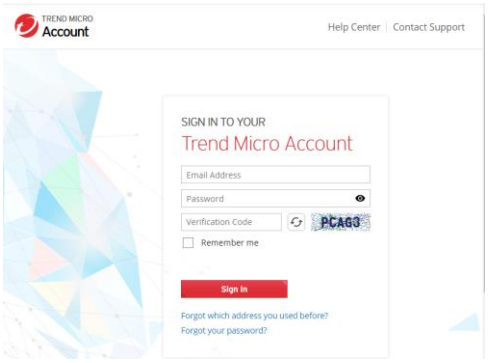



**Figure 402. Trend Micro Account Webpage**

2. In the **Trend Micro Account** page you can sign in to your account, using your **Email Address**, **My Account Password**, and Captcha **Verification Code** if you've already purchased Trend Micro products or services, manage all of your subscriptions in one place, stay up-to-date and protected by getting the latest protection for your devices or those of friends and family, and update your account.

# ID > Subscription Information

**To check your subscription:**

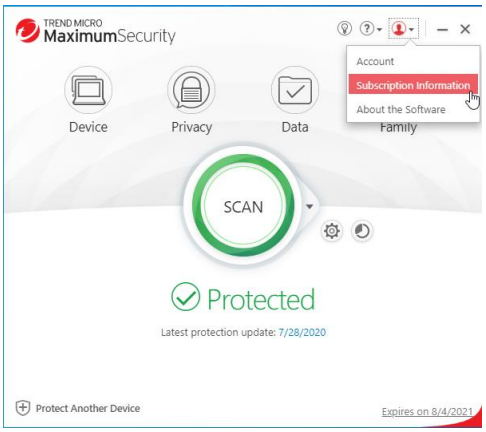



**Figure 403. ID > Subscription Information**

1. Select **ID** (**Identity) > Subscription Information** menu item in the Console. The **Subscription Information** screen appears.

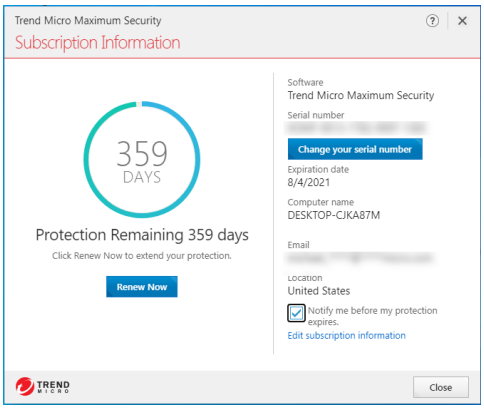



**Figure 404. Subscription Information**

2. In the **Subscription information** screen, you can view the days of protection remaining in your subscription, renew it, view the edition of Trend Micro Security installed on your computer, change your serial number, view your Expiration Date, your Computer Name, the email address the software is registered to, your location, and whether you've chosen to receive the latest news and offers from Trend Micro. Click **Edit subscription information** to edit it.

# ID > About the Software

**To check your software and get updates manually:**

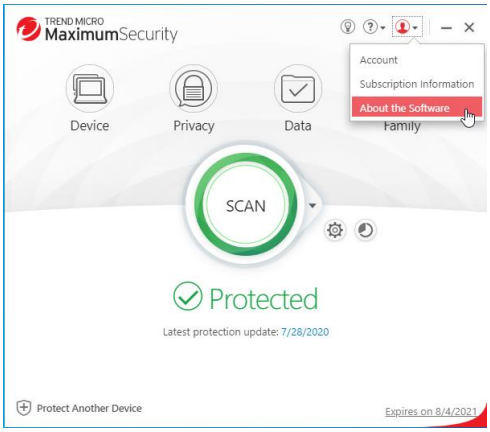



**Figure 405. About the Software**

1. Select the **ID > About the Software** menu item in the Console. The **About the Software** screen appears and automatically queries the Trend Micro servers to provide any available updates of your software.

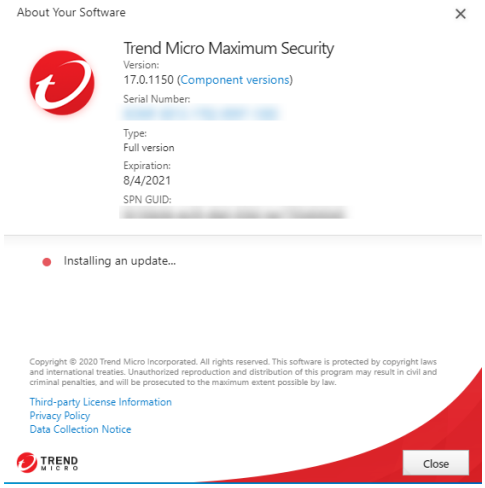



**Figure 406. About Your Software**

2. In the **About Your Software** screen you can view the version of your software and even the version of the components by clicking **Component Versions.**

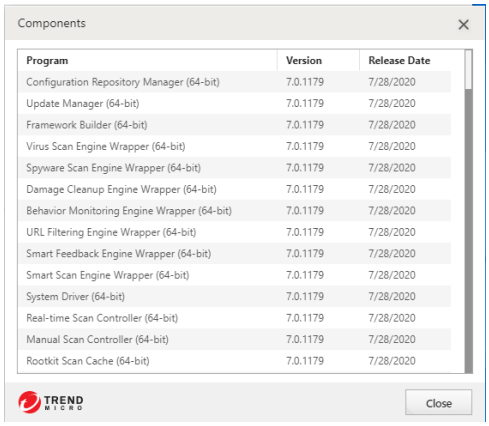



**Figure 407. Component Versions**

3. Click the **Serial Number** link to change it. A screen appears for you to **Enter the Serial Number.**

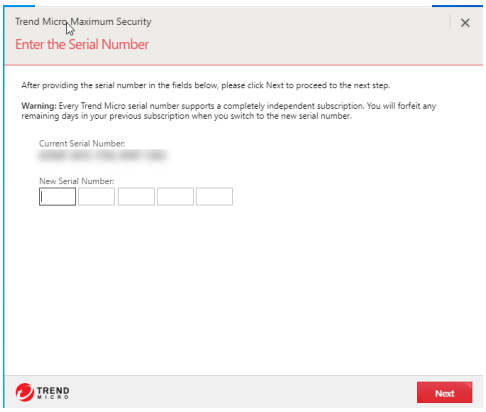



**Figure 408. Enter the Serial Number**

4. Click **Next** to update your software with the new serial number. Your new serial number and its subscription is applied to your software.

# The Trend Micro Tools

The Trend Micro Tools are a set of utilities you can use to perform various functions, from managing your subscription to troubleshooting.

**To use the Trend Micro Tools:**

1. Click **Windows Menu > All Apps** and navigate down to **T** in the menu; then click the Trend Micro menu items for **Trend Micro Security, Trend Micro Password Manager** (Maximum and Premium Security) and **Trend Micro Troubleshooting Tool** to open them.

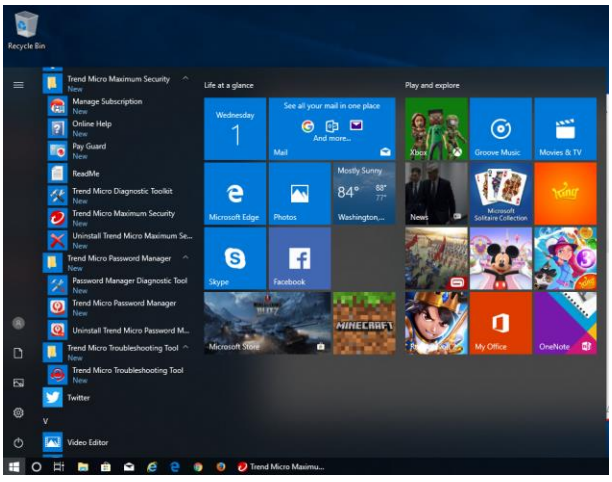


**Figure 409. Trend Micro Utility Menus**

2. Many functions work just as they do from the **Trend Micro Security Console.** Below are brief descriptions of key additional tools.

**Trend Micro Security:**

**Manage Subscription**

1. Click **Manage Subscription** and the **Trend Micro Account** page appears, where you can log into your account to manage your subscription(s).

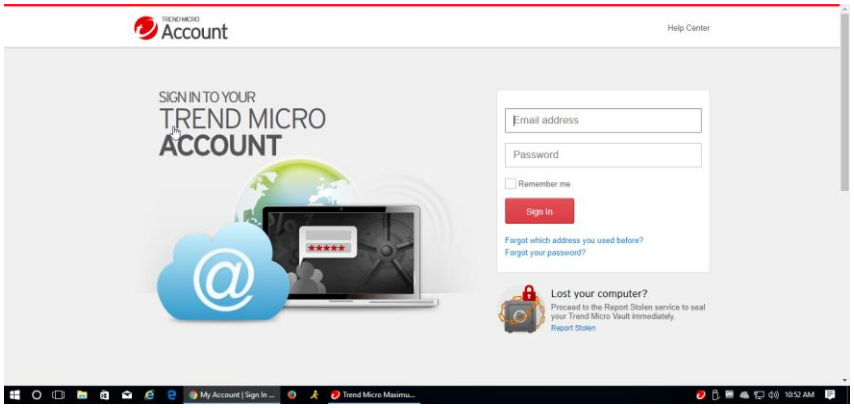



**Figure 410. Manage Subscription > Trend Micro Account**

**Online Help**

1. Click **Online Help** and the **Support** page appears, where you can obtain help about your software

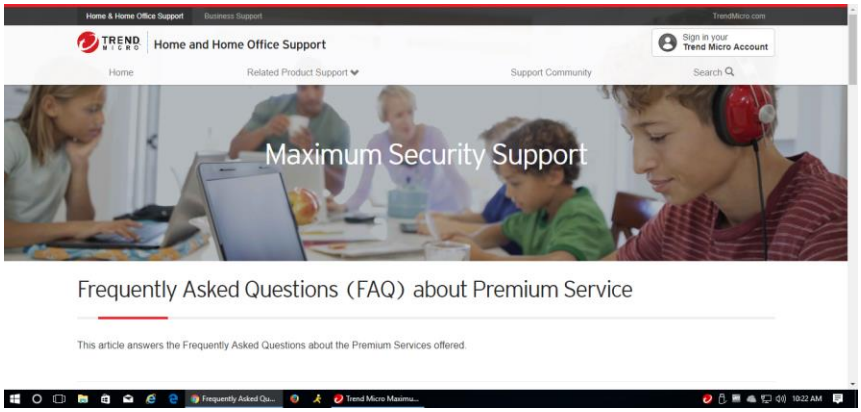



**Figure 411. Support**

**ReadMe**

1. Click the **ReadMe** menu item and choose the document reader you wish to use. The **ReadMe** document appears.

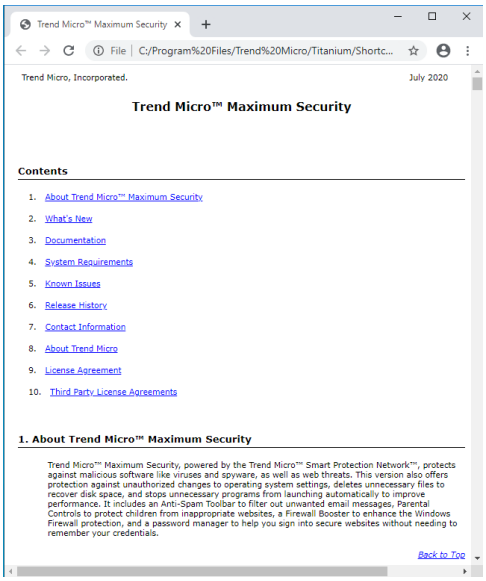



**Figure 412. ReadMe**

2. Click the various items in **ReadMe** to show the contents.

### Trend Micro Diagnostic Toolkit

1. Click **Trend Micro Diagnostic Toolkit** to open it. The **Diagnostic Toolkit** opens.

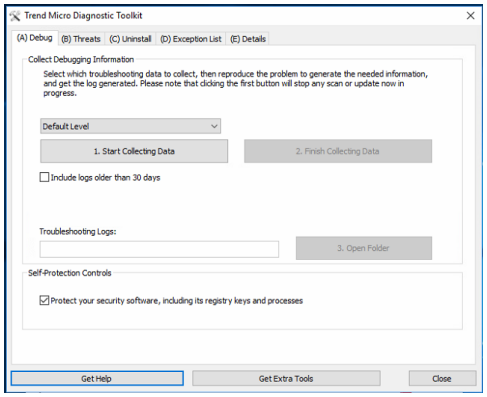



**Figure 413. Trend Micro Diagnostic Toolkit**

2. You'll use the **Diagnostic Toolkit** to help diagnose any problems you may encounter when using Trend Micro Security. These tools include the debugging, uninstall, exception list, and details functions. A Trend Micro Support Specialist will generally work with you to conduct your diagnosis.

### Trend Micro [Edition] Security:

1. Select **Trend Micro [Edition] Security** to launch the Console.

### Trend Micro Pay Guard

1. Click **Trend Micro Pay Guard** and the **Pay Guard** browser launches, to help you bank and shop online securely.

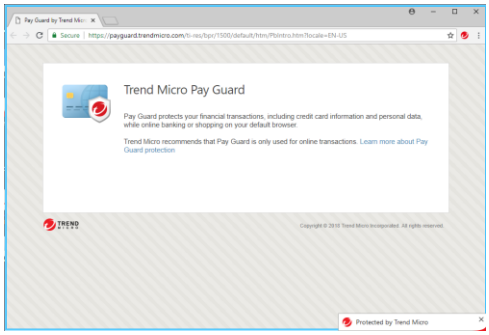



**Figure 414. Trend Micro Pay Guard**

### Trend Micro Password Manager:

### Password Manager Diagnostic Tool

1. Select **Password Manager Diagnostic Tool** to open it.

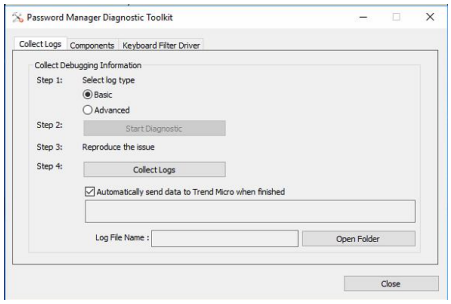



**Figure 415. Password Manager Diagnostic Toolkit**

2. As with Trend Micro Security, the **Password Manager Diagnostic Toolkit** can help you diagnose any problems you may have with Password Manager and is usually used in conjunction with a Trend Micro Support Specialist.

### Trend Micro Password Manager

1. Select **Trend Micro Password Manager** to open the Login webpage for the web console in your default browser.

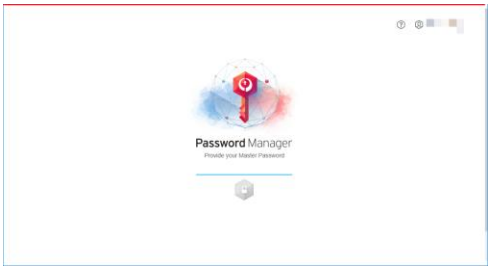



**Figure 416. Password Manager Web Login Page**

### Uninstall Trend Micro Password Manager

1. Select **Uninstall Trend Micro Password Manager** to uninstall the program.

### Trend Micro Troubleshooting Tool:

1. Click **Trend Micro Troubleshooting Tool** to open it.

**Figure 417. Trend Micro Troubleshooting Tool**

2. You use the **Trend Micro Troubleshooting Tool** during a troubleshooting session with a Trend Micro Support Specialist. The specialist will provide you with a **Support Case Token**, which will link the specialist's session directly to your computer.

# About Trend Micro

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables users to enjoy their digital lives safely. For more information, visit www.trendmicro.com.